Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

CONTRATO Nº 014/2023 - AL/AP
PROCESSO N° 0094/2023 – GABCIV - AL/AP

CONTRATO QUE ENTRE SI CELEBRAM A ASSEMBLEIA LEGISLATIVA DO ESTADO DO AMAPÁ E A EMPRESA *NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA*, TENDO POR OBJETO FORNECIMENTO DE 500 (QUINHENTAS) LICENÇA DE SOFTWARE ANTIVÍRUS CORPORATIVO.

A ASSEMBLEIA LEGISLATIVA DO ESTADO DO AMAPÁ - ALAP, com sede na Av. Fab, s/nº, Bairro Central, nesta cidade de Macapá, Estado do Amapá, doravante denominada **CONTRATANTE**, CNPJ nº 34.868.927/0001-60, neste ato representada pelo Diretor Administrativo, Senhor **CEZAR SOUZA DE MELO**, consoante delegação de competência para prática de atos de gestão administrativa e financeira que lhe foi atribuída pela Portaria nº 3053/2023/AL, de 07 de junho de 2023 (DOE/ALAP nº 1547-A, de 07/06/2023), brasileiro, viúvo, advogado, portador da Carteira de Identidade nº 878.24-SSP/AP e do CPF nº 126.083.272-00, residente e domiciliado nesta Capital e a Empresa ***NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA***, CNPJ nº 05.250.796/0001-54, com sede na Av. Pontes Vieira, n°. 2340, Bairro Dionisio Torres, UNO – Medical & Office – Sala 510 à 514 – 5° andar, CEP: 60.135-238, Cidade Fortaleza - CE, Fone (85)3195-2200, e-mail: yure.sabino@networksecure.com.br, doravante denominada **CONTRATADA**, neste ato representada por seu representante legal Yure Leopoldo Sabino de Freitas, RG. nº 559056187 – SSP/SP e do CPF nº 525.285.023-20, residente à Rua Gal Tertuliano Potiguara, n°. 156, apto. 701, Bairro Aldeota, CEP: 60135-280, Cidade de Fortaleza/CE, resolvem celebrar o presente Instrumento Contratual, nos termos da Lei nº 8.666 de 21 de junho de 1993 e alterações, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA: FUNDAMENTO LEGAL:

1.1. Lei nº 10.520, de 17 de julho de 2002;
Lei nº 8.666, de 21 de junho de 1993, e alterações;
Lei Complementar nº 101, de 04 de maio de 2000;
Decreto Lei n° 3.555/2000;
Licitação na Modalidade: PREGÃO Nº 00X/20XX-CPL/AL;
Processo Administrativo nº 0094/2023 - GAVCIV-AL/AP.
Parecer nº: 233/2023-PROGER - AL/AP

CLÁUSULA SEGUNDA: DO OBJETO:

2.1. Contratação de empresa especializada para o fornecimento de licenças de uso de Software antivírus conforme especificação abaixo:

ITEM	ESPECIFICAÇÃO	UND	QUANT	VR. UNT	VR. TOTAL
1	Fornecimento de Licença de uso do software de antivírus **Kaspersky Endpoint Security for Bussiness** com upgrade para ADVANCED, com suporte técnico por 3 (três) anos.	UND	500	R$ 143,00	R$ 71.500,00

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.2. A CONTRATADA deverá garantir a veracidade e legalidade das licenças e o perfeito funcionamento das mesmas, obedecidos os requisitos de qualidade, utilidade e segurança, em conformidade com as normas técnicas relacionadas;
2.3. Este contrato vincula-se às condições e especificações técnicas e quantitativas do Edital, Termo de Referência e na proposta vencedora que embora não transcritos são partes integrantes deste instrumento, no que não o contrarie.
2.4. Requisitos Técnicos
2.4.1. Suporte técnico e garantia do fabricante ou empresa devidamente credenciada e autorizada;
2.4.2. Suporte especializado a ser prestado na modalidade *on-site* (quando necessário), nas dependências do respectivo órgão **CONTRATANTE**, sem prejuízo ao atendimento via remoto/telefone;
2.4.3. Proteção de todos os equipamentos, atuais e novos a serem adquiridos, contra softwares indesejados;
2.4.4. Impedir a disseminação e proliferação de ameaças virtuais;
2.5. Características Técnicas mínimas a serem atendidas
2.5.1. **Servidor de Administração e Console Administrativa**
2.5.1.1 Compatibilidade:
2.5.1.1.1. Microsoft Windows Server 2012/R2 (Todas as edições);
2.5.1.1.2. Microsoft Windows Server 2016 x64;
2.5.1.1.3. Microsoft Windows 8 SP1 Professional / Enterprise 86/x64;
2.5.1.1.4. Microsoft Windows 8/8.1 Professional / Enterprise X86/x64;
2.5.1.1.5. Microsoft Windows 10 (Todas as edições);
2.5.1.1.6 Microsoft Windows 11;
2.5.1.2. Suporta as seguintes plataformas virtuais:
2.5.1.2.1. Vmware: Workstation 16.x Pro, vSphere 6.7, Sphere7;
2.5.1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;
2.5.1.2.3 Citrix XenServer 7.1 LTSR e 8;
2.5.1.3. Características:
2.5.1.3.1. Console deve ser acessada via WEB (HTTPS) ou MMC;
2.5.1.3.2. Console deve ser baseada no modelo cliente/servidor;
2.5.1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
2.5.1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
2.5.1.3.5. Deve permitir incluir usuários do AD para logarem na console de administração;
2.5.1.3.6. Console deve ser totalmente integrada com as suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
2.5.1.3.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
2.5.1.3.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
2.5.1.3.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.1.3.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
2.5.1.3.11. Deve armazenar histórico das alterações feitas em políticas;
2.5.1.3.12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
2.5.1.3.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
2.5.1.3.14. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
2.5.1.3.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
2.5.1.3.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
2.5.1.3.17. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
2.5.1.3.18. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os parâmetros KB/s e horário;
2.5.1.3.19. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução;
2.5.1.3.20. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
2.5.1.3.21. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
2.5.1.3.22. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;
2.5.1.3.23. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
2.5.1.3.24. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
2.5.1.3.25. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
2.5.1.3.26. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
2.5.1.3.27. Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores;
2.5.1.3.28. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
2.5.1.3.29. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
2.5.1.3.30. Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção;
2.5.1.3.31. 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 à proteção;
2.5.1.3.32. Capacidade de, assim que detectar máquinas novas no Active Directory, subredes 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;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.1.3.33. 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 dois dias, etc.;

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

2.5.1.3.35. Deve fornecer as seguintes informações dos computadores: Se o antivírus está instalado; Se o antivírus está iniciado; Se o antivírus está atualizado; Minutos/horas desde a última conexão da máquina com o servidor administrativo; Minutos/horas desde a última atualização de vacinas; Data e horário da última verificação executada na máquina; Se é necessário reiniciar o computador para aplicar mudanças; Data e horário de quando a máquina foi ligada; Quantidade de vírus encontrados (contador) na máquina; Nome do computador; Domínio ou grupo de trabalho do computador; Data e horário da última atualização de vacinas; Sistema operacional com Service Pack; Quantidade de processadores; Quantidade de memória RAM; Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory); Endereço IP; Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido; Atualizações do Windows Updates instaladas; Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD; Vulnerabilidades de aplicativos instalados na máquina;

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

2.5.1.3.37. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: Alteração de Gateway Padrão; Alteração de subrede; Alteração de domínio; Alteração de servidor DHCP; Alteração de servidor DNS; Resolução de Nome; Disponibilidade de endereço de conexão SSL;

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

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

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

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

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

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

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

2.5.1.3.45. Capacidade de gerar traps SNMP para monitoramento de eventos;

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

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

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.1.3.48. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
2.5.1.3.49. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
2.5.1.3.50. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
2.5.1.3.51. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
2.5.1.3.52. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subredes diferentes do servidor;
2.5.1.3.53. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
2.5.1.3.54. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos a outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
2.5.1.3.55. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex.: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
2.5.1.3.56. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
2.5.1.3.57. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
2.5.1.3.58. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
2.5.1.3.59. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo: Nome do vírus; Nome do arquivo infectado; Data e hora da detecção; Nome da máquina ou endereço IP; Ação realizada;
2.5.1.3.60. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
2.5.1.3.61. Capacidade de listar updates nas máquinas com o respectivo link para download
2.5.1.3.62. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
2.5.1.3.63. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
2.5.1.3.64. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
2.5.1.3.65. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
2.5.1.3.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2.5.1.4. Estações Windows

2.5.1.4.1. Compatibilidade:

2.5.1.4.1.1. Microsoft Windows 8 Professional/Enterprise x86 /x64;
2.5.1.4.1.2. Microsoft Windows 8.1 Pro / Enterprise x86 /x64;
2.5.1.4.1.3. Microsoft Windows 10 Pro / Enterprise x86 /x64;
2.5.1.4.1.4. Microsoft Windows Server 2012 R2 Standard x64;
2.5.1.4.1.5. Microsoft Windows Server 2012 Foundation x64;
2.5.1.4.1.6. Microsoft Windows Server 2012 Standard x64;
2.5.1.4.1.7. Microsoft Small Business Server 2011 Standard x64;
2.5.1.4.1.8. Microsoft Windows Server 2016 x64;
2.5.1.4.1.9. Microsoft Windows 11.

2.5.1.4.2. Características:

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.1.4.2.1. Deve prover as seguintes proteções:

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

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

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

2.5.1.4.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc.);

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

2.5.1.4.2.1.6. Firewall com IDS;

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

2.5.1.4.2.1.8. Controle de dispositivos externos;

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

2.5.1.4.2.1.10. Controle de acesso a sites por horário;

2.5.1.4.2.1.11. Controle de acesso a sites por usuários;

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

2.5.1.4.2.1.13. Controle de execução de aplicativos;

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

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

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

2.5.1.4.5. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

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

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

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

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

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

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

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

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

2.5.1.4.13. Capacidade de verificar somente arquivos novos e alterados;

2.5.1.4.14. Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;

2.5.1.4.15. Capacidade de agendar uma pausa na verificação;

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

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

2.5.1.4.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

2.5.1.4.19. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

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

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

2.5.1.4.22. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

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

2.5.1.4.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

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

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

2.5.1.4.27. Deve ter suporte total ao protocolo Ipv6;

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

2.5.1.4.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve: Perguntar o que fazer, ou Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou Permitir acesso ao objeto;

2.5.1.4.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador: Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

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

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

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

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

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

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

2.5.1.4.36. Capacidade de distinguir diferentes subredes e conceder opção de ativar ou não o firewall para uma subrede específica;

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

2.5.1.4.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; Filtragem por aplicativo onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

2.5.1.4.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: Discos de armazenamento locais; Armazenamento removível; Impressoras; CD/DVD; Modems; Dispositivos de fita; Dispositivos multifuncionais; Leitores de smart card; Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc); Wi-Fi; Adaptadores de rede externos; Dispositivos MP3 ou smartphones; Dispositivos Bluetooth; Câmeras e Scanners.

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

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

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

2.5.1.4.43. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.5.1.4.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.5.1.4.45. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

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

2.5.1.4.47. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação: Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.5.1.4.48. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

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

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

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

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

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

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

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

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

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

2.5.1.4.58. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

2.5.2. Estações Mac OS X

2.5.2.1. Compatibilidade:

2.5.2.1.1. MacOS High Sierra 10.13;

2.5.2.1.2. MacOS Sierra 10.12;

2.5.2.1.3. Mac OS X 10.11 (El Capitan);

2.5.2.1.4. Mac OS X 10.10 (Yosemite);

2.5.2.1.5. Mac OS X 10.9 (Mavericks);

2.5.2.2. **Características:**

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

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

2.5.2.2.3. Possuir módulo de bloqueio á ataques na rede;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

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

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

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

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

2.5.2.2.8. Deve possuir suportes a notificações utilizando o Growl;

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

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

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

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

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

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

2.5.2.2.15. Capacidade de verificar somente arquivos novos e alterados;

2.5.2.2.16. Capacidade de verificar objetos usando heurística;

2.5.2.2.17. Capacidade de agendar uma pausa na verificação;

2.5.2.2.18. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou Bloquear acesso ao objeto ou Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);

2.5.2.2.18.1. Caso positivo de desinfecção restaurar o objeto para uso;

2.5.2.2.18.2. Caso negativo de desinfecção Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

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

2.5.2.2.20. Capacidade de verificar arquivos de formato de e-mail;

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

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

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.3. Estações de trabalho Linux 32-64 bits;

2.5.3.1. Compatibilidade

2.5.3.1.1. Ubuntu 18.04, 20.04

2.5.3.1.2. Red Hat® Enterprise Linux® 6.9

2.5.3.1.3. CentOS-6.9

2.5.3.1.4. Debian GNU/Linux 9.4, 10.1, 11.1

2.5.3.1.5. AltLinux 8.0.0

2.5.3.1.6. AltLinux 8.2

2.5.3.1.7. GosLinux 6.6

2.5.3.1.8. Red Hat® Enterprise Linux® 7.4

2.5.3.1.9. CentOS-7.4

2.5.3.1.10. OracleLinux 7.4

2.5.3.1.11. SUSE® Linux Enterprise Server 12 SP5

2.5.3.1.12. OpenSUSE® 42.3

2.5.3.1.13. AltLinux 8.0.0

2.5.3.2. Caracteristica

2.5.3.2.1. Deve prover as seguintes proteções:

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

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

2.5.3.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus;

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

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

2.5.3.2.7. 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;

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

2.5.3.2.9. Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;

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

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

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

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

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

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

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

2.5.3.2.16. Administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.5.4. Servidores Windows 32 ou 64 bits

2.5.4.1. Compatibilidade:

2.5.4.1.1. Microsoft Windows Storage Server SP2 Workgroup Edition;

2.5.4.1.2. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

2.5.4.1.3. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

2.5.4.1.4. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

2.5.4.1.5. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;

2.5.4.1.6. Microsoft Windows Storage Server 2012 (Todas edições);

2.5.4.1.7. Microsoft Windows Storage Server 2012 R2 (Todas edições);

2.5.4.1.8. Microsoft Windows Hyper-V Server 2012;

2.5.4.1.9. Microsoft Windows Hyper-V Server 2012 R2;

2.5.4.1.10. Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;

2.5.4.1.11. Windows Server 2016 Core Standard / Datacenter;

2.5.4.1.12. Windows Storage Server 2016;

2.5.4.1.13. Windows Hyper-V Server 2016.

2.5.5. Características:

2.5.5.1. Deve prover as seguintes proteções:

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

2.5.5.1.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;

2.5.5.1.3 Firewall com IDS;

2.5.5.1.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

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

2.5.5.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); Gerenciamento de tarefa (criar ou excluir tarefas de verificação); Leitura de configurações;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

Modificação de configurações; Gerenciamento de Backup e Quarentena; Visualização de relatórios; Gerenciamento de relatórios; Gerenciamento de chaves de licença; Gerenciamento de permissões (adicionar/excluir permissões acima);

2.5.5.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

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

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

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

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

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

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

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

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

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

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

2.5.5.17. 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;

2.5.5.18. Capacidade de verificar somente arquivos novos e alterados;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

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

2.5.5.20. Capacidade de verificar objetos usando heurística;

2.5.5.21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

2.5.5.22. Capacidade de agendar uma pausa na verificação;

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

2.5.5.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou Bloquear acesso ao objeto; Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);

2.5.5.24.1. Caso positivo de desinfecção restaurar o objeto para uso;

2.5.5.24.2. Caso negativo de desinfecção mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

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

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

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

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

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

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

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

2.5.6. Servidores Linux 32 ou 64 bits

2.5.6.1. Compatibilidade:

2.5.6.1.1. Red Hat® Enterprise Linux® 6.9 Server

2.5.6.1.2. CentOS-6.9

2.5.6.1.3. 1.2.7.1.3 Ubuntu 18.04, 20.04

2.5.6.1.4. Debian GNU / Linux 9.4, 10.1, 11.1

2.5.6.1.5. AltLinux 8.0.0

2.5.6.1.6. AltLinux 8.2

2.5.6.1.7. Red Hat® Enterprise Linux® 7.4 Server

2.5.6.1.8. Red Hat® Enterprise Linux® 7.5 Server

2.5.6.1.9. CentOS-7.4

2.5.6.1.10. CentOS-7.5

2.5.6.1.11. Ubuntu 18.04

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.6.1.12. SUSE® Linux Enterprise Server 12 SP5

2.5.6.1.13. Oracle Linux 7.4

2.5.6.1.14. SUSE® Linux Enterprise Server 12 SP2

2.5.6.1.15. OpenSUSE® 42.3

2.5.6.1.16. Amazon Linux 2

2.5.6.2. Características:

2.5.6.2.1. Deve prover as proteções de Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

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

2.5.6.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar tarefas);

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

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

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

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

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

2.5.6.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção;

2.5.6.2.6. Capacidade de verificar objetos usando heurística;

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

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

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

2.5.7. Smartphones e tablets

2.5.7.1. Compatibilidade:

2.5.7.1.1. Dispositivos com os sistemas operacionais:

2.5.7.1.2. Android 5.0 – 5.1.1 ou superior

2.5.7.1.3. iOS 9.0 – 9.3.5 ou superior

2.5.7.2. Características:

2.5.7.2.1. Deve prover as seguintes proteções:

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.7.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo;

2.5.7.2.1.2. Proteção contra adware e autodialers;

2.5.7.2.1.3. 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;

2.5.7.2.1.4. Arquivos abertos no smartphone;

2.5.7.2.1.5. Programas instalados usando a interface do smartphone

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

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

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

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

2.5.7.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

2.5.7.2.6. Capacidade de desativar por política: Wi-fi; Câmera; Bluetooth.

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

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

2.5.7.2.9. Deverá ter firewall pessoal (Android);

2.5.7.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente;

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

2.5.7.2.12. Capacidade de enviar comandos remotamente de: Localizar; Bloquear.

2.5.7.2.13. Capacidade de detectar Jailbreak em dispositivos iOS;

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

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

2.5.7.2.16. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

2.5.7.2.17. Capacidade de configurar White e blacklist de aplicativos;

2.5.7.2.18. Capacidade de localizar o dispositivo quando necessário;

2.5.7.2.19. Permitir atualização das definições quando estiver em “roaming”;

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

2.5.7.2.21. Deve permitir verificar somente arquivos executáveis; 1.2.8.2.22. Deve ter a capacidade de desinfectar o arquivo se possível;

2.5.7.2.22. Capacidade de agendar uma verificação;

2.5.7.2.23. Capacidade de enviar URL de instalação por e-mail;

2.5.7.2.24. Capacidade de fazer a instalação através de um link QRCode;

2.5.7.2.25. Capacidade de executar as seguintes ações caso a desinfecção falhe: Deletar; Ignorar; Quarentenar; Perguntar ao usuário.

2.5.8. Gerenciamento de dispositivos móveis (MDM)

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.8.1. Compatibilidade:

2.5.8.1.1. Dispositivos com os sistemas operacionais:

2.5.8.1.1.1. Android 5.0 – 5.1.1 ou superior

2.5.8.1.1.2. iOS 9.0 – 9.3.5 ou superior

2.5.8.1.2. Softwares de gerência de dispositivos:

2.5.8.1.2.1. Kaspersky Security Center 10 SP2 MR1 e superior;

2.5.8.1.2.2. Kaspersky Endpoint Security Cloud 3.0 e superior;

2.5.8.1.2.3. VMWare AirWatch 9.2 e superior;

2.5.8.1.2.4. MobileIron 9.6 e superior;

2.5.8.1.2.5. IBM Maas360 10.66 e superior;

2.5.8.1.2.6. SOTI MobiControl 14.1.0 (1152) e superior;

2.5.8.2. Características:

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

2.5.8.2.2. Capacidade de ajustar as configurações de: sincronização de e-mail; uso de aplicativos; senha do usuário; criptografia de dados; conexão de mídia removível.

2.5.8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

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

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

2.5.8.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

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

2.5.8.2.8. Permitir sincronização com perfil do "Touch Down";

2.5.8.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo;

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

2.5.8.2.11. Capacidade de sincronizar com Samsung Knox;

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

2.5.9. Criptografia

2.5.9.1. Compatibilidade

2.5.9.1.1. Microsoft Windows 8/8.1 Enterprise/Pro x86/x64;

2.5.9.1.2. Microsoft Windows 10 Enterprise x86/x64;

2.5.9.1.3. Microsoft Windows 10 Pro x86/x64;

2.5.9.1.4. Microsoft Windows 11;

2.5.9.2. Características

2.5.9.2.1. 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;

2.5.9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

2.5.9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.9.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

2.5.9.2.5. Permitir criar vários usuários de autenticação pré-boot;

2.5.9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

2.5.9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

2.5.9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

2.5.9.2.7.2. Criptografar todos os arquivos individualmente;

2.5.9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

2.5.9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

2.5.9.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

2.5.9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

2.5.9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

2.5.9.2.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;

2.5.9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;

2.5.9.2.13. Bloqueia o reuso de senhas;

2.5.9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;

2.5.9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

2.5.9.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

2.5.9.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

2.5.9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

2.5.9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;

2.5.9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;

2.5.9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

2.5.9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

2.5.9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;

2.5.9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

2.5.9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

2.5.9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

2.5.9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

2.5.9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

2.5.9.2.30. Capacidade de fazer "Hardware encryption".

2.5.10. Gerenciamento de Sistemas

2.5.10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;

2.5.10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

2.5.10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

2.5.10.4. 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;

2.5.10.5. Capacidade de gerenciar licenças de softwares de terceiros;

2.5.10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

2.5.10.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, etc);

2.5.10.8. Possibilita fazer distribuição de software de forma manual e agendada;

2.5.10.9. Suporta modo de instalação silenciosa;

2.5.10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

2.5.10.11. Possibilita fazer a distribuição através de agentes de atualização;

2.5.10.12. Utiliza tecnologia multicast para evitar tráfego na rede;

2.5.10.13. Possibilita criar um inventário centralizado de imagens;

2.5.10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

2.5.10.15. Suporte a WakeOnLan para deploy de imagens;

2.5.10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

2.5.10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

2.5.10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

2.5.10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

2.5.10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
2.5.10.21. Permite baixar atualizações para o computador sem efetuar a instalação;
2.5.10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
2.5.10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
2.5.10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
2.5.10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
2.5.10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
2.5.10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos ou em grupos definidos conforme selecionado pelo administrador;
2.5.10.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
2.5.10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
2.5.10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;
2.5.10.30.1. Capacidade de definir listas de tipos de objetos que não serão verificados;
2.5.10.30.2. Capacidade de definir listas de servidores que não terão o tráfego verificado;
2.5.10.30.3. Capacidade de definir grupos de usuários e aplicar regras de verificação por grupos.

CLÁUSULA TERCEIRA – DO LOCAL DE ENTREGA:
3.1. As licenças de uso dos softwares solicitados deverão ser entregues para utilização, no prazo máximo de 10 (dez) dias uteis, a contar da data de assinatura do CONTRATO;
3.2. A CONTRATADA deverá comunicar, com a antecedência mínima de 02 (dois) dias úteis, ao Gestor do CONTRATO, a data da entrega dos produtos, licenças e serviços;
3.3. A entrega das licenças serão entregues no endereço eletrônico da Diretoria de Tecnologia da Informação da ALAP, e- mail: dirtin@al.ap.leg.br;
3.4. Caso seja verificada qualquer incompatibilidade, as licenças deverão ser substituídos, por conta e ônus da CONTRATADA, em no máximo 02 (dois) dias corridos, não considerados como prorrogação do prazo de execução. Esse processo de verificação de compatibilidade será também comparado com as especificações disponibilizadas pela Contratada, e somente após o cumprimento dessa etapa, será o objeto definitivamente recebido e aceito;
3.5. O recebimento definitivo não excluirá a responsabilidade da CONTRATADA pela perfeita qualidade dos serviços, cabendo-lhe sanar quaisquer irregularidades detectadas, observando o prazo de garantia dos mesmos.

CLÁUSULA QUARTA - DO VALOR DO CONTRATO:
4.1. A Assembleia Legislativa do Estado do Amapá pagará à CONTRATADA, o valor Global de ***R$ 71.500,00*** (setenta e um mil e quinhentos reais)**,** inclusos todas as despesas que resultem no custo do

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

fornecimento dos materiais, tais como impostos, taxas, transportes, seguros, encargos fiscais e todos os ônus diretos e qualquer outras despesas, que incidirem no fornecimento dos materiais e na prestação dos serviços.

CLÁUSULA QUINTA: DAS OBRIGAÇÕES DA CONTRATADA:

5.1. Fornecer os produtos nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste documento;

5.2. Emitir faturas no valor pactuado, apresentando-as ao CONTRATANTE para teste e pagamento.

5.3. Atender prontamente as orientações e exigências inerentes à execução do objeto contratado;

5.4. Assegurar ao CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste termo de referência;

5.5. Não transferir para o CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência;

5.6. Prestar o serviço objeto desta contratação 24 horas por dia, 7 dias por semana, durante todo o período de vigência do contrato, salvaguardados os casos de interrupções programadas;

5.7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE por intermédio de preposto designado para acompanhamento do contrato;

5.8. Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, para realizar as solicitações relativas ao contrato firmado, tais como manutenção, configuração, entre outras;

5.9. Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela CONTRATANTE;

5.10. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.11. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da adjudicação da licitação oriunda deste Termo de Referência.

CLÁUSULA SEXTA: DAS OBRIGAÇÕES DA CONTRATANTE:

6.1. Efetuar o pagamento nas condições e preços pactuados e exigir o fiel cumprimento de todos os requisitos acordados e da proposta apresentada;

6.2. Assegurar os recursos orçamentários e financeiros para custear o contrato;

6.3. Prestar as informações e os esclarecimentos, pertinentes aos eventos, que venham a ser solicitado pela CONTRATADA;

6.4. Promover o acompanhamento e fiscalização da CONTRATADA, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as falhas detectadas, comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da CONTRATADA.

6.5. Instruir os autos do processo administrativo, físico ou eletrônico, conforme o caso, com os

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

documentos afetos ao recebimento provisório e definitivo dos bens, tais como: termo de recebimento provisório e definitivo, devidamente assinados pelo gestor do contrato; metodologia adotada no recebimento definitivo dos bens, contendo a definição da amostra ou a totalidade dos itens a serem testados e inspecionados (exame qualitativo); resultados dos testes de atendimento aos critérios de aceitação e das verificações de conformidade aplicados em cada equipamento avaliado;

6.6. Nomear Gestor e Fiscal do contrato para acompanhar e fiscalizar a execução dos contratos;

6.7.Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

6.8.Observar e fazer cumprir fielmente o que estabelece este Termo de Referência, em particular no que se refere aos níveis de serviço estabelecidos;

6.9. Dirimir as dúvidas que surgirem no curso da prestação dos serviços por intermédio do Gestor ou fiscal do Contrato;

6.10. Notificar a CONTRATADA da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, de acordo com os níveis de serviço estabelecidos;

6.11. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, assegurando à CONTRATADA a ampla defesa e o contraditório;

6.12. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato.

CLÁUSULA SÉTIMA: DA FISCALIZAÇÃO:

7.1. A Diretoria de administração fará a designação de servidor que será responsável pelo acompanhamento da execução e fiscalização do contrato e, igualmente, pelo recebimento e atesto das faturas/Notas Fiscais.

7.2. A Fiscalização será exercida por servidor da Assembleia Legislativa, devidamente designado através de portaria pelo Diretor de Administração, a quem incumbirá acompanhar a execução dos serviços, quando necessário, determinando à Contratada as providências necessárias ao regular e efetivo cumprimento dos serviços, bem como anotar e enquadrar as infrações contratuais constatadas.

7.3. A omissão, total ou parcial, da fiscalização não eximirá a **CONTRATADA** de integral responsabilidade pelos encargos ou serviços que são de sua competência.

7.4. Ao tomar conhecimento de qualquer irregularidade ou de inadimplência por parte da **CONTRATADA**, a fiscalização deverá comunicar, de imediato, por escrito, ao Diretor de Administração, que deverá adotar as providências necessárias para sanar os vícios/pendências apontadas e, se for o caso, responsabilização dos responsáveis.

CLÁUSULA OITAVA: DA DOTAÇÃO ORÇAMENTÁRIA:

8.1. As despesas decorrentes do presente contrato, ficam consignados à conta do orçamento próprio da Assembleia Legislativa do Estado do Amapá – ALAP, no exercício 2023, através da **Unidade Orçamentária** n° 01101 – Assembleia Legislativa do Estado do Amapá; **Ação: 2564** – Coordenação e Apoio das Ações Administrativas e Financeiras; **Natureza da Despesa:** 339039 – Outros Serviços de Terceiros – Pessoa

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

Jurídica; **Fonte de Recursos**: 1500.0000 – Recurso não Vinculado de Imposto.

CLÁUSULA NONA: DO PAGAMENTO:

9.1. Deverá ser fornecida nota fiscal, discriminando de forma detalhada, todo e qualquer registro relacionado com o fornecimento do material, totalizada e discriminada individualmente de forma não contínua, de acordo com a quantidade especificada no item;

9.2. Caso a CONTRATANTE esteja em processo de contestação de alguma(s) Nota(s) Fiscal(is), os pagamentos desta(s) ficará(ão) suspensos e a CONTRATADA ficará impossibilitada de suspender/interromper o fornecimento e de cobrar eventuais juros até a resolução da(s) contestação(s);

9.3. Na contestação a CONTRATADA será notificada, por meio de seu Preposto, de forma pessoal ou por e-mail sobre o descumprimento contratual e a notificação conterá cópia da nota fiscal contestada, uma cópia da parte do contrato com a cláusula descumprida, argumentação e detalhamento das providências a serem tomadas;

9.4. O CNPJ constante da nota fiscal deverá ser o mesmo indicado na proposta e Nota de Empenho.

9.5. O pagamento será autorizado somente após o aceite definitivo da fiscalização.

9.6. Nota Fiscal/Fatura, deverá estar acompanhada:

b) Certidão de regularidade com a Seguridade Social;

c) Certidão de regularidade com o FGTS;

d) Certidão (conjunta) Negativa de Débito Federal;

e) Certidão Negativa de Débito Municipal;

9.7. Atendidas essas exigências e havendo a aceitação/atesto do material pelo servidor responsável, significando esse ato a liquidação da despesa, a fatura será encaminhada, de imediato, à Diretoria de Administração para autorização de pagamento, e após à Diretoria de Orçamento e Finanças para pagamento, o qual ocorrerá em até 5 (cinco) dias úteis, por meio de ordem bancária/transferência, contados da data do aceite.

9.9. Também não serão efetuados quaisquer pagamentos à **CONTRATADA** enquanto houver pendência de liquidação de obrigação financeira em virtude de penalidade que lhe tenha sido regularmente imposta ou de inadimplência contratual e recolhimento dos respectivos encargos sociais;

9.10. Nos casos de eventuais atrasos de pagamento, desde que a LICITANTE vencedora não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo TJMA, entre a data acima referida e a correspondente ao efetivo pagamento da nota fiscal/fatura será calculado por meio da aplicação da seguinte fórmula:

EM = I x N x VP

Em que:

EM = Encargos Moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela pertinente a ser paga;

TX = Percentual da taxa anual = 6% I = Índice de compensação financeira, assim apurado:

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

I = (TX/100) I = (6/100) I = 0,00016438 365 365
365 365

9.11. A **CONTRATANTE**, observados os princípios do contraditório e da ampla defesa, poderá deduzir, cautelar ou definitivamente, do montante a pagar à **CONTRATADA.**

CLÁUSULA DÉCIMA: DA VIGÊNCIA:

10.1. O prazo de vigência do contrato será de 03 (três) anos, a partir de sua assinatura.

10.2. Caso a assinatura do contrato seja eletrônica, considerar-se-á a data da última assinatura.

CLÁUSULA DÉCIMA PRIMEIRA: DA GARANTIA E ASSISTÊNCIA TÉCNICA:

11.1. O fornecedor deverá garantir a autenticidade do produto perante o fabricante.

11.2. A empresa fornecedora do serviço será responsável pela substituição, troca ou reposição dos mesmos se, por ventura, forem entregues com qualquer natureza de falhas ou não compatíveis com as especificações deste Termo de Referência;

11.3. O produto deverá possibilitar a atualização de falhas de segurança, quando disponível;

11.4. O cadastramento do produto junto a fornecedor do software deverá ser em nome da Assembleia Legislativa do Amapá – ALAP e não no nome da contratada.

CLÁUSULA DÉCIMA SEGUNDA: DA QUALIFICAÇÃO TÉCNICA

12.1. A qualificação técnica da Contratada será comprovada mediante a apresentação de, pelo menos, 1 (um) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove o fornecimento do produto, objeto deste Instrumento e do Termo de Referência.

CLÁUSULA DÉCIMA TERCEIRA: DAS SANÇÕES ADMINISTRATIVAS

13.1. O atraso injustificado ou a inexecução total ou parcial do contrato sujeitará a CONTRATADA as sanções administrativas especificadas na Seção II, Capítulo IV, da Lei Federal n°. 8.666/93 (arts. 86 ao 88), conforme estabelecido no instrumento convocatório da licitação ou no contrato.

CLÁUSULA DÉCIMA QUARTA: DO REAJUSTE:

14.1. O valor contratado será fixo e irreajustável.

CLÁUSULA DÉCIMA QUINTA: DA RESCISÃO:

15.1. A inexecução total ou parcial deste Contrato enseja a sua rescisão, observado o contraditório, a ampla defesa e o reconhecimento dos direitos da administração de acordo com o que estabelecem os artigos 77 a 80 da Lei n° 8.666/1993, mediante notificação escrita, através de ofício, entregue diretamente ou por via postal, com aviso de recebimento - AR, sem prejuízo das sanções previstas na CLÁUSULA DÉCIMA TERCEIRA.

CLÁUSULA DÉCIMA SEXTA: DAS DISPOSIÇÕES FINAIS:

16.1. Aplica-se a este Contrato o regime jurídico dos contratos administrativos instituído pela Lei n° 8.666/93 especificamente ao disposto no artigo 58.

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.

Assembleia Legislativa – AP – Divisão de Contratos, Convênios e Inst. Afins
Fl.
Rubrica

16.2. A empresa contratada se obriga a não subcontratar, total ou parcialmente o fornecimento do objeto deste.

CLÁUSULA DÉCIMA SÉTIMA: DO FORO E DA PUBLICAÇÃO:

17.1. Para dirimir quaisquer dúvidas surgidas em decorrência do não cumprimento deste Instrumento, os contratantes elegem o Foro da Cidade de Macapá, com exclusão de qualquer outro, por mais privilegiado que seja, devendo ser publicado o Extrato deste Instrumento, no Diário Oficial Eletrônico da Assembleia Legislativa do Estado do Amapá.

17.2. E assim, por estarem de acordo, ajustados e contratados, após lido e achado conforme, as partes a seguir firmam o presente contrato em 02 (duas) vias, de igual teor e forma, para um só efeito.

Macapá-AP, 20 de dezembro de 2023.

CEZAR SOUZA DE MELO:12626210200

Assinado de forma digital por CEZAR SOUZA DE MELO:12626210200
Dados: 2023.12.26 10:13:46 -03'00'

CEZAR SOUZA DE MELO
Diretor de Administração – AL/AP
CONTRATANTE

ASSINADO DIGITALMENTE
YURE LEOPOLDO SABINO DE FREITAS
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA
Yure Leopoldo Sabino de Freitas
Representante Legal
CONTRATADA

Documento Assinado Eletronicamente nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos.