



Estado do Piauí

Tribunal de Contas



CONTRATO Nº 26/2020/TCE-PI

TERMO DE CONTRATO PARA RENOVAÇÃO DE 650 LICENÇAS DO ANTIVÍRUS KASPERSKY ENDPOINT SECURITYTY CORPORATIVO, INCLUINDO ATUALIZAÇÃO, GARANTIA ESUPORTE TÉCNICO, QUE FAZEM ENTRE SI O TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ E A EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.

O TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ, inscrito no CNPJ/MF sob o nº 05.818.935/0001-01, com sede nesta capital, na Praça Av. Pedro Freitas, nº 2100, bairro São Pedro, CEP 64.018-200, representado por seu Presidente, Conselheiro **ABELARDO PIO VILANOVA E SILVA**, portador do CPF nº 180.496.215-53 e RG 331.172 – SSP/PI, no uso das atribuições legais, adiante denominado simplesmente CONTRATANTE e, de outro, a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**, CNPJ/MF sob o nº 05.250.796/0001-54, sediada na Rua Capitão Melo, 3373, Joaquim Távora, CEP 60.120-220, Fortaleza - CE, telefone (85) 3195-2200/2230/2231 e-mail: licitacoes@networksecure.com.br, neste ato representada pelo gerente geral Sr. **JOSÉ MURILO CIRINO NOGUEIRA JUNIOR**, brasileiro, CPF nº 648.711.503-72, RG nº 99010123694SSP/CE, adiante denominada simplesmente CONTRATADA, firmam o presente contrato, vinculado ao processo TC/011329/2020– Adesão a Ata de SRP 014/2020 - PGJ-CE, pela Lei nº 8.666/93 e suas alterações posteriores, pelo Código Civil Brasileiro, no que couber, especialmente na resolutividade dos casos omissos e pelas cláusulas e condições que seguem abaixo.

1 CLÁUSULA PRIMEIRA – OBJETO

1.1 O objeto do presente contrato é a renovação de 650 licenças do antivírus Kaspersky Endpoint Security Corporativo, incluindo atualizações, garantia e suporte técnico pelo período de 36 (trinta e seis) meses.

1.2 Discriminação do objeto:

1.2.1 As especificações do item contratado são as descritas no quadro abaixo:

ITEM	DESCRIÇÃO DO SERVIÇO	QTD	PREÇO UNITÁRIO (R\$)	PREÇO TOTAL (R\$)
1	Renovação de licenças do antivírus Kaspersky Endpoint Security Corporativo, incluindo atualizações, garantia e suporte	650	108,00	70.200,00



Estado do Piauí

Tribunal de Contas



	técnico pelo período de 36 (trinta e seis) meses. , devendo incluir o suporte técnico remoto (atendimento 8x5).			
--	---	--	--	--

2 CLÁUSULA SEGUNDA – PREÇO

2.1 O valor deste Contrato é de R\$ 70.200,00 (setenta mil e duzentos reais) a ser pago por meio de ordem de crédito na Conta da Contratada nº 789348; Agência 0564; Banco Bradesco.

2.1.1 No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

2.1.2 Os preços dos serviços são fixos e irredutíveis durante o período de vigência da contratação.

3 CLÁUSULA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

3.1 Os recursos financeiros destinados para custear as despesas oriundas deste Contrato serão do Tesouro Estadual, Unidade Orçamentária: 02101; Programa de Trabalho: 01.032. 0017. 4121 - GESTÃO ESTRATÉGICA E MANUTENÇÃO OPERACIONAL; Fonte: 100 - RECURSOS DO TESOIRO ESTADUAL; Natureza: 339040 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

4 CLÁUSULA QUARTA – VIGÊNCIA CONTRATUAL

4.1 A vigência do contrato será de 36 (trinta e seis) meses, contados da sua publicação no Diário Eletrônico do TCE/PI, podendo ter sua vigência prorrogada, até o limite máximo de 48 (quarenta e oito) meses, desde que mantida a obtenção de preços e condições mais vantajosas para a Administração, nos termos do art. 57, inciso IV, da Lei nº 8.666/1.993.

5 CLÁUSULA QUINTA – DETALHAMENTO DO OBJETO CONTRATADO

5.1 Compatibilidade: Versões dos sistemas operacionais a seguir, suas edições, atualizações e versões:

5.1.1 Servidor de Administração e Console Administrativa

a) Microsoft Windows 10 x64;

b) Microsoft Windows Server 2012 R2 x64;

c) Microsoft Windows Server 2016 x64.

d) Microsoft Windows Server 2019 x64.

5.1.2 Cliente para Estações



Estado do Piauí

Tribunal de Contas



a) Microsoft Windows 10 x64;

b) Microsoft Windows 7 x64.

5.1.3 Cliente para Servidores

a) Microsoft Windows Server 2008 R2 x86 / x64;

b) Microsoft Windows Server 2012 R2 x64;

c) Microsoft Windows Server 2016 x64.

d) Microsoft Windows Server 2019 x64.

5.1.4 Plataformas Virtuais

a) VMware: vSphere 6.

5.1.5 Desejável que a solução seja compatível com as futuras versões dos softwares citados anteriormente.

5.2 Funcionalidades Servidor de Administração e Console Administrativa:

5.2.1 A console deve ser acessada via WEB (HTTPS) ou MMC;

5.2.2 A comunicação entre o computador cliente e o servidor de administração deve ser criptografada;

5.2.3 A solução de gerência centralizada deve permitir o monitoramento da implementação, do status de proteção e das atualizações, a visualização de eventos e estatísticas, a configuração de relatórios, o gerenciamento de políticas e tarefas;

5.2.4 Limitar o tráfego de comunicação do cliente com o servidor de administração por subrede por parâmetros de velocidade (KB/s) e horário;

5.2.5 Permitir a atribuição de perfis para os administradores da solução de Antivírus;

5.2.6 Permitir login no console de administração com contas de usuários do Domínio (Active Directory);

5.2.7 Remover remotamente soluções de antivírus (própria ou de terceiros) que estiverem presentes nas estações e servidores da mesma Floresta do servidor de administração;

5.2.8 Instalar remotamente a solução de antivírus nas estações e servidores Windows da mesma Floresta do servidor de administração, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

5.2.9 Registrar as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

5.2.10 Armazenar histórico das alterações feitas em políticas;

5.2.11 Permitir o retorno a 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;

5.2.12 Ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

5.2.13 Informar o número total de licenças gerenciadas;

5.2.14 Verificar qual licença está aplicada para determinado computador;

5.2.15 Monitorar o status de proteção de estações de trabalho e servidores protegidos pela solução antivírus;

5.2.16 Gerar pacotes customizados (auto executáveis) contendo a licença e as configurações do produto;



Estado do Piauí

Tribunal de Contas



- 5.2.17 Selecionar computadores específicos para realizar instalações antes de aplicar nos demais computadores da rede;
- 5.2.18 Criar pacotes com as últimas assinaturas da vacina, de forma que a instalação já contenha as últimas atualizações;
- 5.2.19 Fazer a distribuição remota de outros softwares pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
- 5.2.20 Desinstalar remotamente softwares instalados nos computadores clientes;
- 5.2.21 Realocar máquinas novas na rede para um determinado grupo sem ter o agente instalado, utilizando os seguintes parâmetros:
- 5.2.21.1 Nome do computador;
 - 5.2.21.2 Nome do domínio;
 - 5.2.21.3 Range de IP;
 - 5.2.21.4 Sistema Operacional;
 - 5.2.21.5 Máquina virtual.
- 5.2.22 Importar a estrutura do Serviço de Diretório do Windows (Active Directory) para descobrimento de máquinas;
- 5.2.23 Monitorar diferentes sub-redes de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
- 5.2.24 Monitorar grupos do Serviço de Diretório do Windows (Active Directory) a fim de encontrar equipamentos novos para serem adicionadas a proteção;
- 5.2.25 Ao detectar novos equipamentos no Serviço de Diretório do Windows (Active Directory), sub-redes ou grupos de trabalho, automaticamente importá-los para a estrutura de proteção da console, verificando se possui o antivírus instalado. Caso não possua, deve instalar o antivírus automaticamente;
- 5.2.26 Selecionar equipamentos por características comuns, tais como: versão do sistema operacional, computadores que não tenham o software de proteção instalado, cuja proteção esteja desativada, se físico ou virtual etc;
- 5.2.27 Definir políticas com configurações diferentes por grupos de equipamentos, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 5.2.28 Configurar políticas móveis para que o computador cliente possa, por exemplo, se atualizar via internet quando estiver fora da estrutura de proteção;
- 5.2.29 Fornecer as seguintes informações dos computadores clientes, no mínimo:
- a) Nome, endereço IP e domínio/grupo de trabalho;
 - b) Sistema operacional;
 - c) Se o antivírus está instalado;
 - d) Se o antivírus está em execução;
 - e) Versão do antivírus instalado;
 - f) Se é necessário reiniciar para aplicar mudanças;
 - g) Minutos/horas desde a última conexão com o servidor de administração;
 - h) Minutos/horas desde a última atualização da assinatura da vacina;
 - i) Data da última verificação completa foi executada;
 - j) Quantidade de ameaças encontradas (contador);
 - k) Data e hora da versão do banco de dados da vacina;



Estado do Piauí

Tribunal de Contas



- l) Usuários logados, com dados do contato (conta, email e telefone), caso disponíveis no Serviço de Diretório do Windows (Active Directory);
- m) Aplicativos instalados, inclusive de terceiros;
- n) Informações sobre o hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 5.2.30 Bloquear as configurações do antivírus instalado nas estações e servidores clientes de maneira que o usuário não consiga alterá-las;
- 5.2.31 Permitir a configuração outros servidores administrativos dentro da mesma hierarquia para distribuir carga e otimizar tráfego de rede entre sites diferentes;
- 5.2.32 Fornecer relatórios sobre a estrutura completa da solução de antivírus, considerando todos os servidores de administração que compõem a hierarquia;
- 5.2.33 Capacidade de enviar relatórios e notificações de eventos por e-mail para contas específicas;
- 5.2.34 Permitir a herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 5.2.35 Eleger computadores clientes como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outros computadores clientes irão se atualizar e receber pacotes de instalação, a fim de otimizar o tráfego da rede;
- 5.2.36 Gerar relatórios de hardware e de software dos computadores clientes;
- 5.2.37 Gerar traps SNMP para monitoramento de eventos;
- 5.2.38 Gerar relatórios nos seguintes formatos: PDF, HTML e XLS;
- 5.2.39 Listar os computadores não gerenciados;
- 5.2.40 Baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
- 5.2.41 Função de ligar máquinas via Wake on Lan para execução, por exemplo, de tarefas de verificação e atualização da assinatura da vacina;
- 5.2.42 Habilitar automaticamente uma política caso ocorra uma epidemia na rede, baseado na quantidade de códigos maliciosos encontrados em determinado intervalo de tempo;
- 5.2.43 Verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima da verificação;
- 5.2.44 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;
- 5.2.45 Atualizar de forma incremental as assinaturas das vacinas nos computadores clientes;
- 5.2.46 Armazenar localmente e enviar ao servidor de gerência a ocorrência de códigos maliciosos com os seguintes dados, no mínimo:
 - Nome da máquina ou endereço IP;
 - Nome do arquivo infectado;
 - Data e hora da detecção;
 - Nome do vírus;

• Status.



Estado do Piauí

Tribunal de Contas



5.2.47 Reportar vulnerabilidades de softwares presentes nos computadores clientes;

5.2.48 Listar atualizações dos computadores clientes;

5.2.49 Manter lista centralizada dos arquivos copiados (backup) após modificação ou exclusão nos computadores clientes, para que possam ser salvos, restaurados ou enviados para análise do fabricante a partir de funcionalidade da Console de administração, informando, no mínimo:

- Nome do computador cliente
- Nome do arquivo infectado
- Nome do código malicioso
- Status da infecção
- Data e hora
- Pasta de origem
- Nome do usuário.

5.2.50 Manter lista centralizada dos arquivos possivelmente infectados incluídos na quarentena, para que possam ser salvos, restaurados ou enviados para análise do fabricante a partir de funcionalidade da console de administração, informando, no mínimo:

- Nome do computador cliente
- Nome do arquivo infectado
- Nome do código malicioso
- Status da infecção
- Data e hora
- Pasta de origem
- Nome do usuário.

5.3 Funcionalidades do Software Cliente para Estações Windows:

5.3.1 A solução deve prover pelo menos as seguintes proteções:

- a) Antivírus de Arquivos residente (anti-malware, anti-spyware, anti-trojan) que verifique arquivos criados, acessados ou modificados em tempo real;
- b) Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- c) Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- d) Firewall;
- e) Sistema de detecção de intrusão (IDS);
- f) Autoproteção contra o ataque aos serviços/processos do antivírus;
- g) Controle de dispositivos externos;
- h) Controle de acesso a sites por categoria;
- i) Controle de acesso a sites por horário;
- j) Controle de acesso a sites por usuários;
- k) Controle de acesso à web sites por categoria. Por exemplo, bloqueio de sites com conteúdo de vídeo e áudio;
- l) Controle de execução de aplicativos.

5.3.2 Selecionar os módulos a serem instalados, tanto local quanto remoto;



Estado do Piauí

Tribunal de Contas



- 5.3.3 Permitir a configuração de senha de acordo com a proteção a ser aplicada (Ex: sair do software de proteção, desativar a política, remover a chave de licença);
- 5.3.4 Permitir a atualização da assinatura das vacinas imediatamente após a obtenção junto ao fabricante ou a cada hora;
- 5.3.5 Detectar a presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 5.3.6 Possuir zona de exclusão de pastas e arquivos, a fim de excluí-los da verificação.
- 5.3.7 Possuir lista de exclusão de objetos de acordo com uma classificação, para que seja excluído da verificação;
- 5.3.8 Adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não sejam monitoradas;
- 5.3.9 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 5.3.10 Possibilidade de pausar automaticamente varreduras agendadas, caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 5.3.11 Verificar arquivos por conteúdo, analisando informações de cabeçalho;
- 5.3.12 Fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de constarem na assinatura da vacina;
- 5.3.13 Capacidade de verificar somente arquivos novos e alterados;
- 5.3.14 Capacidade de verificar objetos usando heurística;
- 5.3.15 Capacidade de pausar a proteção em horário específico;
- 5.3.16 Capacidade de pausar a proteção quando um aplicativo for iniciado;
- 5.3.17 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve permitir as seguintes opções:
- a) Desinfectar e excluir em caso de falha;
 - b) Desinfectar e bloquear em caso de falha;
 - c) Bloquear.
- 5.3.18 Realizar backup do objeto antes de qualquer tentativa de desinfecção ou exclusão permanente;
- 5.3.19 Permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 5.3.20 Possibilitar a seleção do tipo de verificação de e-mails, se recebidos e enviados ou somente recebidos;
- 5.3.21 Verificar tráfego nos protocolos POP3, IMAP, NNTP e SMTP;
- 5.3.22 Verificar e-mails usando heurística;
- 5.3.23 Verificar anexos de e-mails do Office;
- 5.3.24 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve permitir as seguintes opções:
- a) Desinfectar e excluir em caso de falha;
 - b) Desinfectar e bloquear em caso de falha;
 - c) Bloquear.
- 5.3.25 Filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 5.3.26 Capacidade de verificar tráfego nos navegadores: Internet Explorer, Firefox e Google Chrome;



Estado do Piauí

Tribunal de Contas



- 5.3.27 Deve ter suporte total ao protocolo IPv6;
- 5.3.28 Possibilidade de alterar as portas monitoradas pelos módulos de proteção contra ameaças de arquivos, web e e-mail;
- 5.3.29 Na verificação de tráfego web, ao encontrar um objeto potencialmente perigoso, deve permitir as seguintes opções:
- Bloquear download;
 - Informar.
- 5.3.30 Possuir lista de exclusão de sites da web, para inclusão de URLs confiáveis que não serão verificadas pelo antivírus de web;
- 5.3.31 Possuir módulo de proteção do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e bloqueadas;
- 5.3.32 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;
- 5.3.33 Possuir módulo de bloqueio de Phishing, com atualizações incluídas nas assinaturas das vacinas;
- 5.3.34 Possuir módulo de IDS (Intrusion Detection System) para proteção contra varredura de portas (port scans) e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com a assinatura das vacinas;
- 5.3.35 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.
- 5.3.36 Distinguir diferentes sub-redes e conceder opção de ativar ou não o firewall para uma sub-rede específica;
- 5.3.37 Possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
- Discos de armazenamento locais;
 - Armazenamento removível;
 - CD/DVD;
 - Impressoras;
 - Câmeras e Scanners
 - Drives de disquete;
 - Modems;
 - Dispositivos de fita;
 - Dispositivos multifuncionais;
 - Leitores de smart card;
 - Dispositivos de sincronização via ActiveSync;
 - Wi-Fi;
 - Adaptadores de rede externos;
 - Dispositivos portáteis;
 - Dispositivos Bluetooth.



Estado do Piauí

Tribunal de Contas



- 5.3.38 Permitir a liberação de acesso a dispositivos específicos por usuário;
- 5.3.39 Permitir a limitação de escrita e leitura em dispositivos de armazenamento externo por usuário e por agendamento;
- 5.3.40 Permitir a configuração de novos dispositivos por Class ID/Hardware ID;
- 5.3.41 Permitir a limitação da execução de aplicativos por hash, 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);
- 5.3.42 Permitir o bloqueio da execução de aplicativos em armazenamento externo;
- 5.3.43 Permitir a limitação do 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;
- 5.3.44 Possibilidade de definir política alternativa caso o computador cliente saia da rede corporativa, na qual as configurações possam ser alteradas, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- 5.3.45 Disponibilizar opção de desempenho para que o computador gerenciado conceda recursos a outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador.
- 5.3.46 Configurar perfis de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- a) Componentes de proteção;
 - b) Controle de dispositivos;
 - c) Controle de aplicativos;
 - d) Zona de confiança;
 - e) Prevenção de intrusão de host;
 - f) Controle de web.
- 5.4 **Funcionalidades do Software Cliente para Servidores Windows:**
- 5.4.1 Prover pelo menos as seguintes proteções:
- a) Antivírus de Arquivos residente (anti-malware, anti-spyware, anti-trojan) que verifique arquivos criados, acessados ou modificados em tempo real;
 - b) Autoproteção contra o ataque aos serviços/processos do antivírus;
 - c) Firewall;
 - d) Sistema de detecção de intrusão (IDS).
- 5.4.2 Permitir a seleção dos módulos a serem instalados, tanto local quanto remoto;
- 5.4.3 Permitir a atualização da assinatura das vacinas imediatamente após a obtenção junto ao fabricante ou a cada hora;
- 5.4.4 Configurar perfis de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- a) Componentes de proteção
 - b) Controle de dispositivos
 - c) Controle de aplicativos
 - d) Zona de confiança
 - e) Prevenção de intrusão de host
- 5.4.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos e escopo de regras de rede;



Estado do Piauí

Tribunal de Contas



b) Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo terá acesso a rede.

5.4.6 Definir a quantidade máxima 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;

5.4.7 Bloquear malwares tais como Cryptlockers;

5.4.8 Recuperar automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc), informando a quantidade de tentativas de recuperação;

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

5.4.10 Criar e configurar logs de acordo com o componente de proteção e a criticidade;

5.4.11 Configurar níveis de verificação diferentes por disco, fixo e removível, pasta, grupo de pastas, arquivo e compartilhamento de rede;

5.4.12 Permitir o desbloqueio automático após tempo determinado do acesso ao servidor protegido por máquinas bloqueadas por apresentaram atividade maliciosa;

5.4.13 Capacidade de criar uma lista de máquinas que nunca serão bloqueadas mesmo quando infectadas;

5.4.14 Identificação de antivírus de outros fabricantes instalados que possam causar incompatibilidade;

5.4.15 Configurar adicionar discos, fixos e removíveis, pastas, arquivos, compartilhamentos de rede em uma zona de exclusão, a fim de excluí-los da verificação;

5.4.16 Adicionar processos confiáveis à zona confiável, a fim de excluí-los da verificação.

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

5.4.18 Verificar arquivos por conteúdo, analisando informações de cabeçalho;

5.4.19 Capacidade de verificar somente arquivos novos e alterados;

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

5.4.21 Capacidade de verificar objetos usando heurística;

5.4.22 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

5.4.23 Capacidade de agendar uma pausa na verificação;

5.4.24 Ao encontrar um objeto potencialmente perigoso, a proteção em tempo real deve permitir as seguintes opções:

a) Notificar;

b) Bloquear o acesso, permitindo a execução de ações preestabelecidas pelo administrador);

c) Executar ações de acordo com o tipo de malware detectado.

5.4.25 Realizar backup do objeto antes de qualquer tentativa de desinfecção ou exclusão permanente;

5.4.26 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena e definição do limite de armazenamento;



Estado do Piauí

Tribunal de Contas



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

5.4.28 Possuir módulo de monitoramento de scripts, para prevenir atividades maliciosas.

5.5 Dinâmica de Execução

5.5.1 O prazo para entrega das licenças será de até 15 (quinze) dias corridos, contados da data de assinatura do contrato;

5.5.2 A instalação de qualquer software que faça parte das soluções contratadas será de responsabilidade do fornecedor, cabendo a este inclusive fornecer suporte técnico, caso necessário;

5.5.3 As credenciais de acesso ao site do fabricante devem ser particulares do Contratante para acesso à área exclusiva do site, visando a verificação das licenças disponibilizadas;

5.6 Instrumentos de Solicitação do(s) Serviço(s)

5.6.1 Um canal de suporte técnico através de serviço telefônico será disponibilizado pela contratada através de um número de telefone gratuito (0800 ou ligação com custo de local) a um Centro de Atendimento por Voz, com atendimentos obrigatoriamente na língua portuguesa, devendo esse Centro operar de forma ininterrupta, no mínimo, das 8h às 18h em dias úteis (8x5);

5.6.2 Um canal de suporte técnico através de Portal web e/ou correio eletrônico (e-mail), deverá ser disponibilizado pela contratada de forma ininterrupta 24x7(vinte e quatro horas por dia, sete dias por semana).

5.6.3 Os chamados técnicos deverão possuir identificador de ocorrência próprio, data e hora de abertura devidamente repassada ao CONTRATANTE, a fim de registro e acompanhamento das ocorrências;

5.6.4 A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento das ocorrências;

5.6.5 Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações:

- A. N° do chamado;
- B. Categoria de prioridade;
- C. Descrição do problema e da solução;
- D. Procedimentos realizados;
- E. Data e hora da abertura e do fechamento do chamado;
- F. Data e hora do início e do término da execução dos serviços; e
- G. Identificação do técnico da empresa.

5.6.6 Os tempos de resposta e de solução para os chamados técnicos abertos serão contados a partir do seu registro, através de contato telefônico ou por outro meio disponível.

5.6.7 Em caso de atraso na conclusão do atendimento, em qualquer nível de prioridade, será admitida a proposição, pela CONTRATADA, de justificativa técnica, a qual deverá conter os motivos do atraso, acompanhada da devida comprovação;

5.6.8 A justificativa eventualmente apresentada será analisada pela Administração a qual emitirá parecer, para fins de aceitação ou não da justificativa;



Estado do Piauí

Tribunal de Contas



5.6.9 Em sendo aceita, ocorrerá tão somente a interrupção dos prazos contratuais, sem prejuízo da conclusão do chamado. Em não sendo aceita, impor-se às sanções previstas na forma da execução contratual, bem como no Item Penalidades deste Contrato;

5.6.10 A justificativa deverá ser apresentada em até 03 (três) dias úteis após a conclusão do chamado. Uma vez apresentada fora deste prazo, caberá a Administração conhecer ou não o documento;

5.7 Níveis de Serviços Exigidos (NSE)

5.7.1 Os chamados técnicos serão classificados pelo Fiscal Técnico, por criticidade, de acordo com o impacto no ambiente computacional, conforme abaixo:

- a) **Nível 1:** Perda total de um serviço essencial e não é possível dar continuidade ao trabalho de maneira razoável;
- b) **Nível 2:** Perda ou degradação significativa dos serviços.;
- c) **Nível 3:** Perda ou degradação moderada dos serviços, mas o trabalho pode razoavelmente continuar de maneira prejudicada.

5.7.2 Os serviços de suporte e assistência técnica em garantia deverão atender, respectivamente, os seguintes prazos de solução do incidente:

- a) Os chamados de Nível 1 deverão ser atendidos em até 2(duas) horas, contado da validação do chamado, e solucionados em até 6 (seis) horas do início do atendimento;
- b) Os chamados de Nível 2 deverão ser atendidos em até 8(oito) horas e solucionados em até 12 (doze) horas a contar do início do atendimento;
- c) Os chamados de Nível 3 deverão ser atendidos em até 12 (doze) horas e solucionados em até 24 (vinte e quatro) horas a contar do início do atendimento, podendo serem realizados de forma remota, se for possível;

5.7.3 Os chamados poderão ser escalados pelo Fiscal Técnico para níveis mais altos ou mais baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de solução serão automaticamente ajustados, a partir da notificação de mudança, para o novo nível de prioridade;

5.8 Direitos de Propriedade Intelectual

5.8.1 Os conhecimentos técnicos repassados para a equipe técnica do TCE-PI serão utilizados em casos de interrupção, transição e encerramento contratual, de modo a minimizar impactos e permitir que as necessidades do Tribunal não sejam prejudicadas ou interrompidas;

5.8.2 A CONTRATADA cederá ao Tribunal de Contas do Estado do Piauí, nos termos do artigo 111 da Lei nº 8.666/93, concomitante com o art. 4º da Lei nº 9.609/1998, o direito patrimonial e a propriedade intelectual em caráter definitivo dos sistemas desenvolvidos e resultados produzidos em consequência do cumprimento deste contrato, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, fluxogramas e documentação didática, em papel ou mídia eletrônica.

5.9 Qualificação Técnica dos Profissionais

5.9.1 A CONTRATADA encaminhará a relação nominal dos técnicos capacitados para execução dos serviços, desde que prestados diretamente pela contratada, contendo a



Estado do Piauí

Tribunal de Contas



indicação dos perfis exigidos, acompanhada dos currículos individuais e credenciais e/ou certificados que comprovem sua qualificação técnica nos equipamentos e/ou serviços contratados. A lista deverá ser encaminhada ao fiscal do contrato no **prazo máximo de 72 horas após a assinatura do contrato**;

5.9.2 Tais documentos deverão ser encaminhados à Diretoria de Informática - DTIF;

5.9.3 Durante a execução do objeto da licitação, sempre que houver alteração da relação de técnicos, a CONTRATADA deverá remeter à DTIF, em até 3 dias úteis antes do efetivo envio dos novos técnicos, lista atualizada, bem como currículos e cópias dos certificados e documentos relativos aos novos técnicos incluídos na lista;

5.9.4 O Tribunal analisará a documentação recebida, de acordo com as especificações técnicas deste Termo, podendo solicitar a substituição dos profissionais que não possuam as qualificações mínimas exigidas para o perfil;

5.9.5 Apenas os técnicos formalmente indicados pela CONTRATADA podem ser alocados para execução dos serviços, exceto em situações excepcionais mediante anuência prévia do Tribunal;

5.9.6 Para cumprir todas as atividades previstas, a CONTRATADA deverá empregar esforços de técnicos treinados e certificados pelo fabricante dos produtos, visando uma atuação mais eficiente e a perfeita execução dos serviços ora contratados;

5.9.7 A CONTRATADA deverá indicar um profissional para Gerenciamento do Projeto e que ficará sendo o ponto focal de comunicação entre a mesma e o TCE-PI.

5.9.8 Todas as atividades de implantação serão realizadas obrigatoriamente por profissionais devidamente capacitados pelos fabricantes e indicados pela CONTRATADA sendo esta condição devidamente comprovada;

5.9.9 A comprovação do vínculo profissional formal dos técnicos com a CONTRATADA deverá ser feita mediante apresentação de um dos seguintes documentos:

5.9.10 No caso de vínculo empregatício: cópia da Carteira de Trabalho e Previdência Social (CTPS), expedida pelo Ministério do Trabalho, contendo as folhas que demonstrem o número de registro e qualificação civil;

5.9.11 No caso de vínculo societário: ato constitutivo da empresa devidamente registrado no órgão de Registro de Comércio competente, do domicílio ou da sede do licitante;

5.9.12 No caso de profissional autônomo: contrato de prestação de serviços;

5.9.13 Outros documentos hábeis à comprovação do vínculo profissional.

6 CLÁUSULA SEXTA - DO PRAZO PARA EXECUÇÃO DO OBJETO

6.1 O prazo para entrega das licenças será **de até 15 (quinze) dias corridos**, contados da data de assinatura do contrato.

7 CLÁUSULA SÉTIMA - RECEBIMENTO DO OBJETO

7.1 A Contratada deverá disponibilizar para o Contratante o download dos softwares objeto do contrato, incluindo toda documentação técnica atualizada, tais como: especificações, manuais, guias de instalação, de operação, de diagnósticos, de solução de problemas e outros pertinentes.



Estado do Piauí

Tribunal de Contas



7.2 O objeto será **recebido provisoriamente**, no dia da disponibilização das subscrições e do respectivo download dos softwares, para verificação da conformidade com as especificações constantes deste Contrato.

7.3 O Termo de **Recebimento Definitivo** será emitido pela Equipe de Planejamento da Aquisição em até 10 (dez) dias úteis contados da data de recebimento do Termo de Recebimento Provisório.

7.4 O recebimento do objeto contratado será realizado dentro do expediente do TCE-PI, no intervalo das 7h às 14h, dias úteis;

8 CLÁUSULA OITAVA - ACOMPANHAMENTO E FISCALIZAÇÃO

8.1 O acompanhamento e fiscalização da execução do contrato serão exercidos pelos fiscais do contrato, especialmente designados para este fim, que deverão informar ao gestor do contrato as ocorrências durante seu andamento;

8.2 Compete ao gestor e aos fiscais do contrato dirimir eventuais dúvidas que surgirem no curso da sua prestação e de tudo dar ciência à empresa CONTRATADA, para fiel execução contratual durante toda a vigência do contrato, de acordo com os termos do Art. 67 da Lei nº 8.666/93;

8.3 Sem prejuízo da plena responsabilidade da empresa CONTRATADA perante o TCE-PI ou a terceiros, os serviços estarão sujeitos à mais ampla e irrestrita fiscalização;

8.4 A presença do servidor designado como gestor do contrato e dos servidores designados como fiscais do contrato não diminuirá a responsabilidade contratual da empresa CONTRATADA.

8.5 O Contrato será acompanhado e fiscalizado por servidor (fiscal) lotado na Divisão de Redes e Segurança do TCE/PI, designado especialmente para tal fim, o qual fiscalizará a execução dos serviços, observando-se o exato cumprimento de todas as cláusulas e condições contratuais, determinando quando necessário, a regularização de falhas observadas, cabendo ao referido servidor o “ATESTO” das respectivas Notas Fiscais, conforme prevê o art. 67 da lei 8.666/93 e Resolução TCE/PI nº 28 de 03/11/2016 – publicado do Diário Oficial Eletrônico nº 207/16 de 08/11/2016.

9 CLÁUSULA NONA – DAS CONDIÇÕES DE PAGAMENTO

9.1 O **pagamento** do objeto contratado efetivamente fornecido será efetuado mediante ordem de crédito em conta corrente da Contratada, indicada na sua proposta e dar-se-á em parcela única no prazo máximo de **até 30 (trinta) dias corridos**, contados a partir da data do recebimento definitivo do objeto e após solicitação de pagamento no Setor de Protocolo do TCE-PI, devidamente instruído com os seguintes documentos, nos termos do art. 63 da Lei nº 4.320/1964:

a) Requerimento de pagamento contendo no mínimo a qualificação do credor (dados básicos, data e assinatura do representante legal), o valor requerido e a competência a que se refere;

b) Nota de Empenho (cópia);

c) Nota Fiscal atestada pelo fiscal do contrato;



Estado do Piauí

Tribunal de Contas



- d) Comprovantes da entrega do material e/ou da prestação efetiva do serviço;
- e) Cópia do contrato e aditivos (se for o caso): caso inexistir, apresentar Ata de Registro de Preço e Ordem de Fornecimento dos serviços prestados e/ou dos materiais fornecidos.
- f) Certidões de Regularidade Fiscal e Trabalhista constante do art. 29 da Lei nº 8.666/93;
- g) Declaração do Sistema de Cadastramento Unificado de Fornecedores (SICAF) ou documentos aptos a substituir as referidas certidões nele mencionadas;
- h) Comprovação da condição de optante do SIMPLES: apenas credores optantes;
- i) Outros documentos contratualmente exigidos: o credor deve verificar particularidades estabelecidas no instrumento contratual como relatórios, comprovantes de cumprimento de obrigações tributárias, previdenciárias, trabalhistas ou outros.

9.2 Nenhum pagamento será efetuado à contratada, enquanto pendente de liquidação de qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência contratual, sem que isso gere direito a acréscimos de qualquer natureza.

9.3 O desconto de qualquer valor no pagamento devido ao contratado será precedido de processo administrativo em que será garantido à empresa o contraditório e a ampla defesa, com os recursos e meios que lhes são inerentes.

9.4 Do pagamento serão descontadas as despesas com seguros, transportes, fretes, tributos, encargos trabalhistas e previdenciários e demais despesas envolvidas na execução do objeto que correrão por conta da CONTRATADA.

9.5 A empresa optante pelo Simples Nacional deverá encaminhar juntamente a Nota Fiscal Eletrônica/DANFE, sempre que houver fornecimento, declaração em conformidade com o Art. 6º da Instrução Normativa SRF nº 1.234/2012.

9.6 Se a nota fiscal apresentar irregularidades, falhas ou omissões que comprometam a liquidação da despesa, ou a contratada não apresentar todas as condições de habilitação, o prazo supracitado será contado a partir da data em que tais impropriedades forem sanadas.

9.7 Nos casos de eventuais atrasos de pagamento, desde que a licitante vencedora não tenha concorrido de alguma forma para tanto, incidirão correção monetária e juros moratórios. Fica convencionado que a correção monetária e os encargos moratórios devidos pelo Tribunal de Contas do Estado do Piauí entre a data acima referida e a do efetivo pagamento da nota Fiscal/fatura será calculada por meio da aplicação da seguinte fórmula: $EM = I \times N \times VP$, onde:

9.7.1 EM = Encargos moratórios;

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

9.7.3 VP = valor da parcela em atraso

9.7.4 I = índice de compensação financeira = 0,00016438, assim apurado:

9.7.5 $I = i/365$ $I = 0,06/365$ $I = 0,00016438$

9.7.6 onde: I = taxa percentual no valor de 6%.

9.8 A correção monetária será calculada com a utilização do índice IGP-M da Fundação Getúlio Vargas



Estado do Piauí

Tribunal de Contas



9.9 É vedada expressamente a realização de cobrança de forma diversa da estipulada neste documento, em especial a cobrança bancária, mediante boleto ou mesmo o protesto de título, sob pena de aplicação das sanções previstas neste instrumento e indenização pelos danos decorrentes.

9.10 O desconto de qualquer valor no pagamento devido ao contratado será precedido de processo administrativo em que será garantido à empresa o contraditório e a ampla defesa, com os recursos e meios que lhes são inerentes

9.11 É vedado ao contratado transferir a terceiros os direitos ou créditos decorrentes do contrato.

9.12 Não haverá, em hipótese alguma, pagamento antecipado.

9.13 Os casos omissos obedecerão ao previsto no Art. 73 e da Lei Nº 8.666/93.

10. CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE

10.1 Designar os servidores que atuarão como fiscais do contrato que deverão:

10.1.1 Informar ao gestor do contrato se os prazos foram cumpridos pela empresa CONTRATADA e demais fatos que achar relevante para a perfeita gestão do contrato;

10.1.2 Tanto a comissão de recebimento como os fiscais do contrato devem cumprir integralmente o que for determinado por meio de qualquer acordo, termo de compromisso ou qualquer outro documento expedido pelo TCE-PI, sem comprometimento das obrigações estabelecidas neste Contrato.

10.2 Proporcionar todas as condições necessárias, além daquelas sob responsabilidade da Equipe de Gestão do Contrato, para que a CONTRATADA possa cumprir seus deveres;

10.3 Fiscalizar, com o auxílio da área técnica, o cumprimento, por parte da CONTRATADA, das exigências legais e de eficiência, eficácia, efetividade e economicidade do contrato.

10.4 Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da CONTRATADA conforme determina a lei, antes de efetuar o pagamento devido.

10.5 Proceder às advertências, multas e demais cominações legais pelo descumprimento das obrigações assumidas pela CONTRATADA.

10.6 Liquidar o empenho e efetuar o pagamento à CONTRATADA, do valor resultante da execução dos serviços, consoante às condições estabelecidas neste Contrato.

11 CLÁUSULA DÉCIMA PRIMEIRA – OBRIGAÇÕES DA CONTRATADA

11.1 Entregar as licenças adquiridas no Tribunal de Contas do Estado do Piauí, localizada na Av. Pedro Freitas, 2100, Centro Administrativo, CEP: 64018-900, Teresina-PI;

11.2 Fornecer suporte técnico, pelo período de duração do contrato, contados do recebimento definitivo das licenças;

11.3 Disponibilizar central de atendimento via telefone (0800 ou com custo de ligação local) e meio eletrônico para realização de requisições de execução de serviço ou resolução de dúvidas durante 5 (cinco) dias por semana, 8 (oito) horas por dia, prevalecendo a especificação de cada item;



Estado do Piauí

Tribunal de Contas



11.4 Conceder acesso ao controle de atendimento ao TCE-PI, para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Tribunal;

11.5 Para todo o objeto do contrato apresentar, no ato da assinatura do contrato, declaração do fabricante dos softwares ou do distribuidor autorizado no Brasil, com menção ao edital ou ao Tribunal de Contas do Piauí, afirmando que a licitante está apta a comercializar e prestar assistência técnica em seus produtos e que os itens cotados possuem garantia e assistência técnica, a ser prestada no Estado do Piauí e autorizada pelo fabricante.

11.6 Fornecer o licenciamento dos produtos acompanhado de chaves de ativação e demais itens necessários à sua perfeita instalação e funcionamento, contemplando as versões indicadas no Edital ou as versões mais recentes disponibilizadas pelo fabricante, observando todas as especificações técnicas consignadas em sua proposta comercial.

11.7 Fornecer credenciais de acesso ao(s) site(s) do fabricante, para a realização de “downloads” dos produtos adquiridos, em suas versões mais recentes, bem como para a realização de “downloads” de correções, atualizações recentes, drivers, e quaisquer “softwares” de apoio ali disponibilizado.

11.8 Disponibilizar ao Contratante monitor de controle de licenças fornecidas e dos direitos adquiridos, cuja atualização de informações ficará a seu cargo ou do próprio fabricante.

11.9 Validar, sempre que necessário, em razão de eventuais mudanças de nomenclatura dos produtos, os novos nomes e códigos referentes às versões mais atualizadas.

11.10 Fornecer a documentação técnica completa e atualizada dos produtos adquiridos, contendo manuais do fabricante, guias de instalação e outros documentos pertinentes, sempre em suas versões originais;

11.11 A documentação poderá ser disponibilizada em site do fabricante, com acesso liberado ao Contratante.

11.12 Disponibilizar ao Contratante acesso, sem quaisquer ônus adicionais, ao site que contenha Base de Conhecimento do fabricante sobre os produtos contemplados no objeto do ajuste;

11.13 Manter, durante todo o período de vigência do contrato, todas as condições que ensejaram sua contratação.

11.14 Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do CONTRATANTE.

11.15 Manter sigilo, sob pena de responsabilidade civil e penal, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato, devendo orientar seus empregados nesse sentido.

11.16 Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:

11.16.1 À política de segurança adotada pela CONTRATANTE e as configurações de hardware e de softwares decorrentes;

11.16.2 Ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;



Estado do Piauí

Tribunal de Contas



11.16.3 Ao processo de implementação, no ambiente da CONTRATANTE, dos mecanismos de criptografia e autenticação;

11.17 Comunicar ao Contratante, por escrito, qualquer anormalidade verificada na entrega dos produtos, fornecendo os devidos esclarecimentos, sempre que solicitados.

11.18 Cumprir, sem ônus adicionais ao Contratante, todas as cláusulas contratuais que definam suas obrigações.

11.19 Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e nas orientações da Contratante, observando sempre os critérios de qualidade aplicáveis.

11.20 Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do Contrato, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, todas as obrigações e responsabilidades, sem qualquer ônus adicional ao TCE/PI.

11.21 A CONTRATADA é obrigada a aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, e desde que formalizados durante a vigência do contrato.

12 CLÁUSULA DECIMA SEGUNDA – DA SUBCONTRATAÇÃO

12.1 Não Será admitida a subcontratação do objeto desta licitação.

13 CLÁUSULA DÉCIMA TERCEIRA – DAS E PENALIDADES

13.1 A CONTRATADA ficará sujeita às seguintes penalidades, com fundamento nos artigos 86 e 87 da Lei nº. 8.666/93, sem prejuízo das responsabilidades civil e criminal, assegurada prévia e ampla defesa:

13.1.1 O atraso injustificado na entrega do objeto sujeitará a CONTRATADA à multa diária de 0,03% (três centésimos por cento), sobre o valor da parcela inadimplida, a título de multa de mora;

13.1.2 O atraso injustificado no cumprimento dos demais prazos estipulados sujeitará a CONTRATADA à multa diária de 0,03% (três centésimos por cento), sobre o valor da parcela inadimplida contratado, a título de multa de mora.

13.1.3 O atraso injustificado no cumprimento dos demais prazos estipulados, sujeitará a CONTRATADA à multa por hora em atraso de 0,03% (três centésimos por cento), sobre o valor da parcela inadimplida, a título de multa de mora;

13.2 Pela inexecução total ou parcial do contrato, a Administração poderá, nos termos do art. 87 da Lei n. 8.666/1993, garantida a prévia defesa, aplicar ao contratado as seguintes sanções:

a) Advertência;



Estado do Piauí

Tribunal de Contas



b) Multa:

I - compensatória diária de 0,03% (três centésimos por cento), sobre o valor contratado, caso haja a interrupção/ suspensão dos serviços de garantia e/ou suporte técnico;

II – compensatória de 10% (dez por cento), sobre o valor da parcela inadimplida;

c) Suspensão temporária;

d) Declaração de Inidoneidade;

13.2 A inexecução total ou parcial do contrato poderá acarretar a sua rescisão, conforme previsto no Contrato e nos art. 77 a 80 da Lei n. 8.666/1993.

13.3 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente, a Lei nº 9.784, de 1999.

13.4 As penalidades serão devidamente autuadas via protocolo administrativo interno.

13.5 A multa, aplicada após regular processo administrativo, será descontada da garantia prestada. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente.

13.6 Não será aplicada multa se, comprovadamente, o atraso na execução do objeto advier de caso fortuito ou motivo de força maior, entendido dessa forma pela Administração.

13.7 As penalidades serão obrigatoriamente registradas no SICAF.

14.0 CLÁUSULA DÉCIMA QUARTA - DO ACORDO DE NÍVEL DE SERVIÇO E SUPORTE TÉCNICO

14.1 O tempo de garantia de atualização das licenças e o suporte técnico será de 36 (trinta e seis) meses.

14.2 O serviço de suporte deverá ser prestado diretamente pela contratada, nos casos eventuais de dúvidas ou suporte técnico, no que diz respeito a incidentes e problemas relacionados ao objeto.

14.3 Na abertura do chamado de suporte e garantia a CONTRATANTE informará a contratada a categoria de prioridade, que poderá ser baixa, normal ou alta.

14.4 Os prazos para primeira resposta do atendimento dos chamados e prazo para solução deverão seguir o estabelecido no Quadro 01 do ACORDO DE NÍVEL DE SERVIÇO – ANS, abaixo discriminado:

	PRIORIDADE BAIXA	PRIORIDADE NORMAL	PRIORIDADE ALTA
PRAZO PARA PRIMEIRA RESPOSTA	12 horas	08 horas	02 horas
PRAZO PARA SOLUÇÃO	24 horas	12 horas	06 horas



Estado do Piauí

Tribunal de Contas



14.5 Das multas previstas nos casos em que houver o descumprimento do ANS:

14.5.1 A violação do acordo de nível de serviço – ANS pela contratada, conforme indicado no quadro 01, acarretará a aplicação de multas. Nos casos em que ocorrer descumprimento do ANS, serão aplicadas multas de acordo com o quadro 02 (grau de correspondência) e conforme o tipo de infração no quadro 03:

Quadro 02

GRAU	CORRESPONDÊNCIA
1	1,0% sobre o valor total do contrato
2	5,0% sobre o valor total do contrato
3	10,0% sobre o valor total do contrato
4	20,0% sobre o valor total do contrato

Quadro 03

ITEM	INFRAÇÃO	GRAU	INCIDÊNCIA
1	Exceder em até 2 horas o tempo previsto para solução dos chamados técnicos do ANS.	1	Por chamado
2	Exceder em entre 2 horas a 4 horas o tempo previsto para solução dos chamados técnicos do ANS.	2	Por chamado
3	Exceder em mais de 8 horas o tempo previsto para solução dos chamados técnicos do ANS	3	Por chamado
4	Exceder em mais de 3 ocorrências as infrações 1, 2 ou 3	4	Por evento

14.6 Todas as ocorrências do ANS serão verificadas mensalmente por meio de relatório enviado pela contratada, contendo os registros dos chamados eventualmente abertos pela SETIN. O relatório da empresa será confrontado pelos registros internos da SETIN para fins de validação. Havendo ocorrências que se configurem em qualquer tipo das infrações do quadro 03, a SETIN encaminhará o relatório para a CAILC (Comissão de Apuração de Infrações em Licitações e Contratos), devidamente assinado pelo gestor do contrato para abertura de procedimento de aplicação de multas.

14.7 No processo de aplicação de multas é assegurado o direito ao contraditório e à ampla defesa, facultada defesa prévia do interessado no prazo de 10 (dez) dias úteis contados da respectiva intimação.



Estado do Piauí

Tribunal de Contas



- 14.8 As multas decorrentes das infrações supramencionadas poderão ser cumulativas e os demais casos de inadimplementos de suas obrigações estarão sujeitos as sanções legais conforme o item 14 deste instrumento.

15 CLÁUSULA DECIMA QUINTA - PREÇO, REAJUSTE E ALTERAÇÕES.

15.1 O objeto será contratado pelo preço licitado será fixo e irreajustável pelo período de 36 (trinta e seis) meses, quando então se promoverá a sua correção de acordo com a variação do Índice de Preços ao Consumidor Amplo – IPCA, em conformidade com a legislação em vigor, tomando-se por base o índice vigente no mês de apresentação da proposta ou do orçamento a que essa se referir;

15.2 O preço ajustado já leva em conta todas e quaisquer despesas incidentes na execução do objeto, tais como frete, tributos, transporte, entre outros;

15.3 O preço ajustado também poderá sofrer correção desde que reste comprovada a ocorrência de quaisquer das hipóteses previstas na alínea “d”, do inciso II, do art. 65, da Lei nº 8.666/93.

15.4 Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666/93.

15.5 A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais os acréscimos ou supressões que se fizerem necessários até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16 CLÁUSULA DÉCIMA SEXTA – RESCISÃO

16.1 A rescisão desta contratação se dará nos termos dos artigos 79 e 80 da Lei nº 8.666/93.

16.2 No caso de rescisão provocada por inadimplemento da CONTRATADA, o TCE/PI poderá reter, cautelarmente, os créditos decorrentes do contrato até o valor dos prejuízos causados, já calculados ou estimados.

16.3 A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

16.4 No procedimento que visa à rescisão do contrato, será assegurado o contraditório e a ampla defesa, sendo que, depois de encerrada a instrução inicial, a CONTRATADA terá o prazo de 5 (cinco) dias úteis para se manifestar e produzir provas, sem prejuízo da possibilidade de o TCE/PI adotar, motivadamente, providências acauteladoras.

17 CLÁUSULA DÉCIMA SÉTIMA – VEDAÇÕES

17.1 É vedado à CONTRATADA:

17.1.1 caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

17.1.2 interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.



Estado do Piauí

Tribunal de Contas



18 CLÁUSULA DECIMA OITAVA – DOS CASOS OMISSOS.

18.1 Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002, Decreto nº 10.024 de 20 de setembro de 2019 e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

19 CLÁUSULA DÉCIMA NONA – PUBLICAÇÃO

19.1 Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial Eletrônico do TCE/PI, no prazo previsto na Lei nº 8.666, de 1993.

20 CLÁUSULA VIGÉSIMA – FORO

20.1 É eleito o Foro da Comarca de Teresina para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Teresina (PI), 08 de outubro de 2020.

(assinado digitalmente)

Conselheiro Abelardo Pio Vilanova e Silva
Presidente do TCE-PI

(assinado digitalmente)

José Murilo Cirino Nogueira Junior
Representante Legal da Contratada

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal de Assinaturas Certisign. Para verificar as assinaturas clique no link: <https://www.portaldeassinaturas.com.br/Verificar/E175-DD01-A231-219A> ou vá até o site <https://www.portaldeassinaturas.com.br:443> e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: E175-DD01-A231-219A



Hash do Documento

2CCF033B5355780CA036C4F412F50EFA865017E5B613F805F8A9600AC5D98EB7

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 08/10/2020 é(são) :

☒ José Murilo Cirino Nogueira Junior (Signatário) - 648.711.503-72 em 08/10/2020 16:04 UTC-03:00

Tipo: Assinatura Eletrônica

Identificação: Por email: licitacoes@networksecure.com.br

Evidências

Client Timestamp Thu Oct 08 2020 16:04:54 GMT-0300 (-03)

Geolocation Latitude: -3.764454908612822 Longitude: -38.48887166148135 Accuracy: 65

IP 191.34.236.64

Assinatura:



Hash Evidências:

98D28E3D91FBFC2222DF4982BDAB3F2CAAD050A639F17E4A1D7A461C8F2E6F45

