



CONSELHO REGIONAL DE MEDICINA DO ESTADO DO TOCANTINS

TERMO DE REFERÊNCIA (TR)

Palmas-TO, 02 de julho de 2026

TERMO DE REFERÊNCIA

LICITAÇÃO E CONTRATAÇÃO DIRETA

(Processo Administrativo nº 25.27.000005403-8)

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para prestação de serviços gerenciados e continuados de segurança da informação, contemplando o fornecimento, em regime de comodato, de soluções de proteção de rede e dados, juntamente com serviços técnicos especializados para implantação, gerenciamento e suporte às soluções de TIC, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE ÚNICO	Item	Especificação	CATSER	Métrica ou Unidade de Medida	QTD	Valor Unit./mês	Valor Total
	1	SERVIÇOS DE GERENCIAMENTO DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC) - SERVIÇOS TÉCNICOS ESPECIALIZADOS DE IMPLANTAÇÃO	27014	serviço/horas	36	n/a	R\$ 695,04
	2	SERVIÇOS DE GERENCIAMENTO DE REDES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC) -- SERVIÇOS GERENCIADOS DE FIREWALL	26999	serviços/mês	1	R\$ 1.761,68	R\$ 21.140,20

	3	SERVIÇOS ESPECIALIZADOS DE DISPONIBILIZAÇÃO DE CÓPIAS DE SEGURANÇA DE DADOS (BACKUP COMO SERVIÇO) - SERVIÇOS GERENCIADOS DE BACKUP	27758	serviços/mês	4	R\$ 1.003,92	R\$ 12.047,04
	4	SERVIÇOS ESPECIALIZADOS DE DISPONIBILIZAÇÃO DE CÓPIAS DE SEGURANÇA DE DADOS (BACKUP COMO SERVIÇO) - SERVIÇOS DE ARMAZENAMENTO PARA BACKUP (TB)	27758	serviços/mês	6	R\$ 2.403,62	R\$ 28.843,44
					TOTAL:		R\$ 62.725,72

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como **comum (ns)**, conforme justificativa constante do Estudo Técnico Preliminar.

Classificação do objeto quanto ao modelo de execução

1.3. O serviço é enquadrado como continuado tendo em vista que será prestado mensalmente durante toda a vigência contratual, sendo a vigência anual mais vantajosa considerando o Estudo Técnico Preliminar.

Prazo de vigência

1.4. O prazo de vigência da contratação é de 12 (doze) meses contados a partir da data de assinatura do Contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.5. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se devido ao Conselho Regional de Medicina do Estado do Tocantins (CRM-TO) enfrentar um desafio relevante em segurança da informação. Sua infraestrutura tecnológica reúne numerosos computadores e servidores que armazenam grandes volumes de dados e sustentam sistemas essenciais à operação institucional. A ausência de mecanismos de proteção adequados expõe esses ativos a ameaças cibernéticas, como malware, ataques de rede, ransomware e acessos indevidos, com potencial de ocasionar indisponibilidade de serviços, vazamento ou perda de informações. Fundamenta-se na necessidade imperativa de garantir a segurança da informação do Conselho Regional de Medicina do Estado do Tocantins (CRM-TO), cuja infraestrutura tecnológica

armazena dados sensíveis e sustenta sistemas essenciais à operação institucional

Para preservar a confidencialidade, a integridade e a disponibilidade das informações, bem como resguardar os ativos corporativos, torna-se indispensável a adoção de medidas capazes de mitigar riscos e evitar danos de natureza tecnológica, financeira e reputacional. A manutenção de um ambiente seguro exige não apenas tecnologias robustas, mas também processos maduros e equipe especializada, com capacidade de resposta contínua.

A implementação integral desses requisitos de forma exclusivamente interna demandaria investimentos substanciais em hardware, software, processos e capacitação, além de estrutura para monitoramento contínuo. Esse nível de complexidade e custo torna a internalização plena antieconômica e operacionalmente desafiadora.

Diante desse contexto, opta-se pela contratação de fornecedor especializado para a gestão da segurança da informação. Essa abordagem viabiliza a adoção de soluções avançadas de proteção, com monitoramento por profissionais capacitados, reduz a sobrecarga da equipe técnica interna e permite que ela se concentre nas atividades principais da instituição.

O projeto justifica-se, assim, pela necessidade de fortalecer o CRM-TO com soluções integradas de segurança da informação, garantindo vigilância constante diante de ameaças conhecidas e emergentes e diminuindo a carga administrativa associada à proteção de redes, endpoints e dados.

Os serviços de backup gerenciado contemplarão a transferência de dados para datacenter externo, elevando significativamente a segurança e a resiliência das informações. Essa medida supera limitações do armazenamento local e reduz o risco de perda total em eventos de desastre, como incêndios ou falhas críticas.

Portanto, a adoção combinada de soluções robustas de firewall e backup, aliada à gestão especializada em segurança da informação, constitui medida estratégica para elevar o nível de proteção do ambiente tecnológico do CRM-TO, mitigar riscos e aumentar a eficiência operacional, assegurando um ambiente mais protegido, estável e preparado para os desafios atuais e futuros.

Do Diagnóstico da Necessidade: O cenário atual apresenta um desafio relevante caracterizado pela ausência de mecanismos de proteção adequados, o que expõe os ativos de TIC a ameaças cibernéticas como ransomware, malware e acessos indevidos. Tais ameaças representam riscos concretos de indisponibilidade de serviços públicos, vazamento de dados sigilosos e danos reputacionais à autarquia.

Da Escolha da Solução Mais Vantajosa: Conforme demonstrado no Estudo Técnico Preliminar (ETP) anexo a este processo, foram analisadas diferentes alternativas para satisfazer essa necessidade, incluindo a aquisição de ativos (hardware/software) com gestão própria versus a contratação de serviços gerenciados. A análise comparativa concluiu que a contratação de empresa especializada para prestação de Serviços Gerenciados de Segurança (MSS), englobando Firewall e Backup em lote único, representa a solução técnica e economicamente mais vantajosa para a Administração.

Esta escolha justifica-se pois:

Economicidade: Elimina o alto custo inicial de investimento (CAPEX) em aquisição de equipamentos que sofrem rápida obsolescência e reduz custos com capacitação continuada de equipe interna.

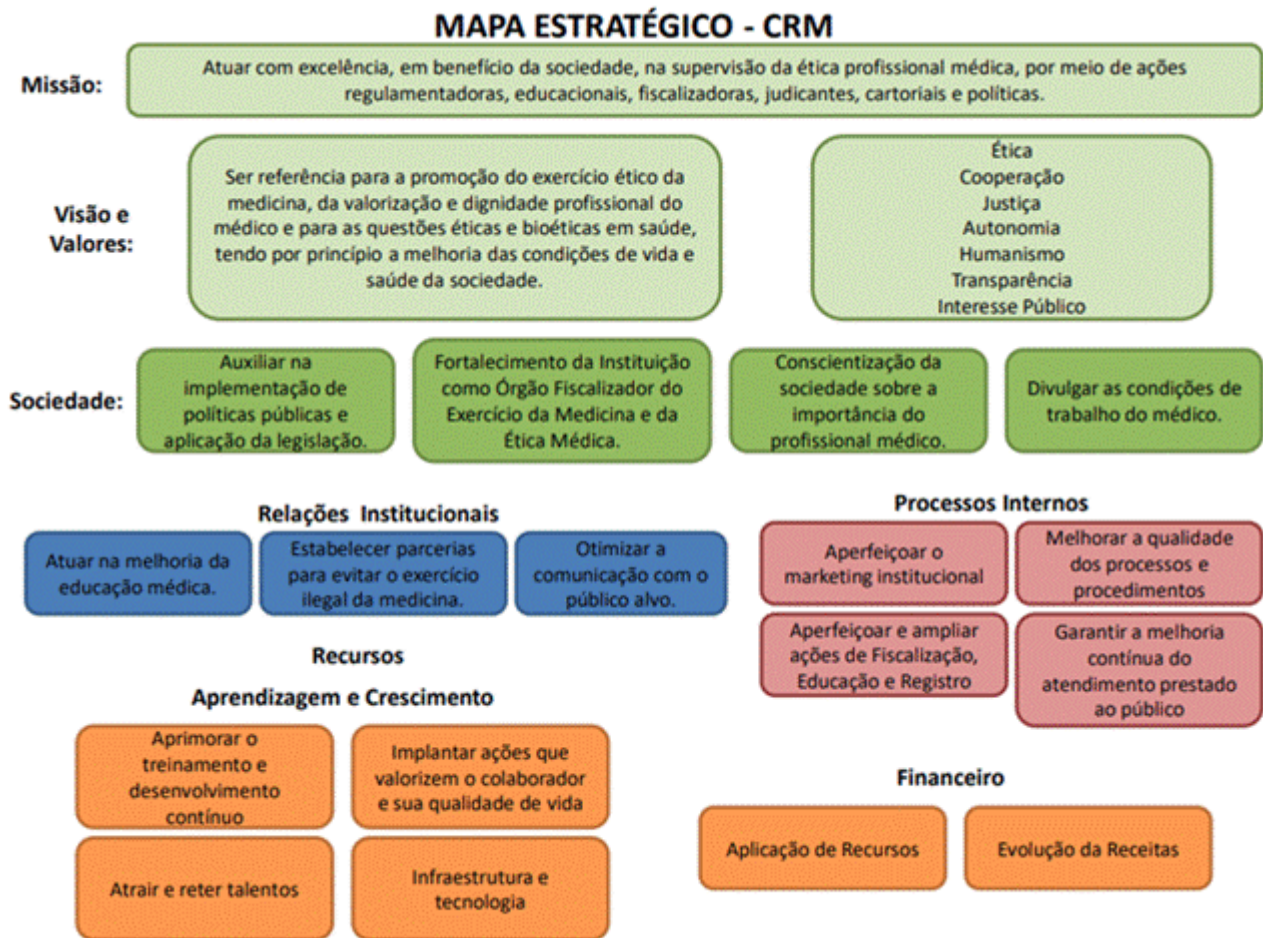
Eficiência Técnica: Garante acesso imediato a tecnologias de ponta e monitoramento especializado 24/7, superando as limitações operacionais da equipe interna reduzida.

Benefícios Esperados: Assegura a continuidade do negócio, a conformidade com a Lei Geral de Proteção de Dados (LGPD) e a integridade das informações médicas e administrativas.

Desta forma, a contratação alinha-se aos objetivos estratégicos do CRM-TO e atende aos requisitos de governança de TIC, provendo uma resposta eficaz aos riscos identificados no planejamento.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme consta das informações básicas deste termo de referência.

2.3. O objeto da contratação também está alinhado com o Planejamento Estratégico do CRM-TO:



2.4. Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste em fornecer segurança de dados, continuidade operacional e proteção contra ameaças cibernéticas, como ataques de malware, intrusões e acessos não autorizados.

FIREWALL

Proteção contra acessos não autorizados: Atua como um filtro que impede acessos indesejados da internet e controla quais dados podem entrar e sair da rede do órgão.

Prevenção contra ameaças avançadas: Firewalls de Próxima Geração (NGFW) oferecem funcionalidades como detecção e prevenção de intrusão (IPS), análise de tráfego encriptado, controle de aplicações e proteção baseada em inteligência artificial.

Monitoramento e controle: Permite o controle avançado de acesso de usuários e a análise de tráfego para identificar atividades maliciosas, ajudando a cumprir a legislação de segurança e privacidade de dados.

Centralização de segurança: Soluções como o UTM (Unified Threat Management) centralizam diversas funções de segurança em um único dispositivo, como antivírus, VPN e filtragem de conteúdo, facilitando o gerenciamento.

BACKUP

Continuidade do serviço: Garante que o órgão possa se recuperar rapidamente de perdas de dados causadas por falhas técnicas, ataques de ransomware ou outros incidentes, mantendo a continuidade das operações.

Recuperação de dados: Assegura que as informações possam ser restauradas de forma confiável e eficiente após um incidente, preservando dados essenciais.

Integridade e conformidade: Protege a integridade dos dados e ajuda a garantir o cumprimento de requisitos legais e regulatórios sobre a retenção e a privacidade das informações.

Proteção contra ransomware: O backup regular e seguro é uma das principais defesas contra ataques de ransomware, pois permite a restauração dos dados sem a necessidade de pagar resgate.

Itens por quantidade:

	Item	Especificação	Métrica ou Unidade de Medida	QTD
LOTE	1	SERVIÇOS TÉCNICOS ESPECIALIZADOS DE IMPLANTAÇÃO	serviço/horas	36
	2	SERVIÇOS GERENCIADOS DE FIREWALL	serviços/mês	1
	3	SERVIÇOS GERENCIADOS DE BACKUP	serviços/mês	4
	4	SERVIÇOS DE ARMAZENAMENTO PARA BACKUP (TB)	serviços/mês	6

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

DAS ATIVIDADES DE SUPORTE, GERENCIAMENTO E MONITORAMENTO

- A CONTRATADA deverá prover os serviços objetos deste Termo de forma remota por meio da Central de Serviços e presencialmente, quando necessário;
- A CONTRATADA deverá ter estrutura de suporte para atendimento presencial em Palmas - TO;
- Os serviços de suporte técnico devem contemplar as seguintes ações e/ou premissas:
- Recepcionar via telefone ou e-mail, e registrar corretamente à abertura de qualquer chamado técnico referente à solução;
- Implantar e manter scripts de atendimento adequados às necessidades de suporte técnico do Contratante;
- Implantar e manter base de conhecimento adequada às necessidades de suporte técnico do Contratante;
 - Solucionar problemas ou sanar dúvidas por telefone e/ou e-mail quanto aos questionamentos repassados pelo Contratante;
 - Acionar equipes específicas da CONTRATADA para realizar a reposição antecipada de equipamentos defeituosos, quando for necessário;
 - Realizar, mediante aviso e agendamento com o Contratante, atualização de softwares e firmwares dos produtos ofertados, quando disponibilizado pelo fabricante;
 - Agendar visitas de manutenção corretiva com o Contratante, registrando chamados para este fim;
 - Acompanhar os chamados desde sua abertura até seu encerramento, independente de existir ou não redirecionamento para outras equipes técnicas da própria CONTRATADA ou Fabricante.

FAZEM PARTE DO ESCOPO DO SUPORTE TÉCNICO, DURANTE SUA VIGÊNCIA, OS SEGUINTE SERVIÇOS:

- Disponibilizar atualizações de softwares e firmwares dos serviços/produtos ofertados sem qualquer tipo de ônus para o CONTRATANTE;
- Realizar visita local para manutenção preventiva dos produtos instalados na sede do CONTRATANTE em horário programado junto ao CONTRATANTE;
- Realizar a reposição antecipada de qualquer equipamento que apresentar defeito dentro do prazo de 48h (quarenta e oito horas) após abertura de chamado ou constatação da necessidade de troca, sendo que a reposição deverá ocorrer na sede do CONTRATANTE;
- A reposição antecipada deve ocorrer durante o período necessário em que o equipamento do CONTRATANTE estiver em conserto, ficando a cargo da CONTRATADA todo ônus de retirada, conserto e devolução;
- A reposição antecipada também deve ser feita por um ou mais equipamentos que somados sejam iguais ou similares ao equipamento defeituoso, com relação às características físicas e lógicas, e sem que haja nenhum tipo de prejuízo ao funcionamento do ambiente do CONTRATANTE;
- Os serviços de suporte técnico devem estar disponíveis em horário integral 24/7 durante sua vigência.
- Para os serviços de suporte técnicos, a CONTRATADA deverá possuir Central de Serviços disponibilizando contato por telefone, e-mail e ferramenta web para abertura e acompanhamento dos chamados em tempo integral 24/7;
- Caberá a Central de Serviços ser o contato único entre a CONTRATADA e a CONTRATANTE, registrando todas as solicitações e registros de ocorrência em sistema eletrônico específico para este, além de fornecer ao CONTRATANTE o número de identificação da ocorrência para acompanhamento. A Central de Serviços deverá disponibilizar software web para abertura de chamados e acompanhamento dos mesmos.

ATIVIDADES DE GERENCIAMENTO, MONITORAMENTO E SUPORTE.

Gerais:

- A CONTRATADA deverá realizar a gestão e o monitoramento dos equipamentos, softwares e serviços que forem ofertados. Os serviços deverão ser prestados remotamente, a partir de um Centro de Operação de Segurança da CONTRATADA, estritamente de acordo com as especificações deste documento;
- Os serviços de gestão, monitoramento e suporte deverão ser realizados pela CONTRATADA, na modalidade de tempo integral 24/7;
- A CONTRATANTE deverá possuir acesso de leitura aos equipamentos que forem utilizados para possibilitar o serviço, através de consoles de gerenciamento;
- O gerenciamento e suporte remoto dos equipamentos deverá ser feito via VPN ou Console de Gerenciamento;

Firewall:

- Realizar, via solução de Firewall especificada a proteção da rede, controle de acessos à internet e aplicativos, priorização de serviços, conforme políticas de segurança definidas juntamente com a CONTRATANTE;
- Atualização de patches e novas versões de firmware;
- Inclusão/exclusão/alteração de regras nos equipamentos de Firewall, com análise crítica a fim de garantir a gestão de mudanças no ambiente da CONTRATANTE;
- Identificar brechas e vulnerabilidades na configuração de regras implantadas e propor, de forma contínua, melhorias na proteção do ambiente, sempre que identificado a necessidade;
- Realizar o monitoramento contínuo das seguintes atividades:
- Intrusões detectadas pelos módulos de IPS e antivírus do equipamento de Firewall ofertado;
- Indisponibilidade do cluster de Firewall;
- Análise e monitoramento de tráfego;
- Indisponibilidade de VPN;
- Indisponibilidade dos links de Internet;
- Sobrecarga de processamento;
- A CONTRATADA deverá disponibilizar, mensalmente, até o 5º dia útil do mês posterior à prestação de serviços, através de e-mail ou via impressa, os seguintes relatórios de utilização dos últimos 30 (trinta) dias:
 - Domínios mais acessados;
 - Relatório de malwares detectados;
 - Relatório de tentativas de intrusão.

Backup Profissional:

- Realizar, via solução de backup especificada a proteção completa (sistema operacional, aplicativos instalados, configurações e dados), diário e/ou intervalos pré-determinados, automaticamente, dos servidores e computadores críticos da CONTRATANTE;
- Realizar a análise do ambiente atual da CONTRATANTE (identificando modo de operação) e efetuar ajustes no ambiente de backup caso necessário;
- Prestar todo o suporte técnico necessário para a perfeita execução do backup e/ou sua restauração e configuração;
- Realizar a recuperação (restauração) dos dados (da base de dados completa ou apenas arquivos específicos) sempre que demandado pela CONTRATANTE e sem custos adicionais;
- Trafegar os dados entre os servidores protegidos e o Datacenter externo (onde serão armazenados), com padrões de Segurança (ex: Criptografia, etc.);
- Propor, de forma contínua, melhorias no sistema de backup, sempre que identificado a

necessidade;

- Atualização de patches e novas versões de software;
- Monitorar o backup diário de dados, alertando em casos de falhas, pouco espaço em disco ou erros de qualquer natureza e propor e/ou realizar a imediata correção;
- A CONTRATADA deverá disponibilizar, mensalmente, até o 5º dia útil do mês posterior à prestação de serviços, através de e-mail ou via impressa, os seguintes relatórios de utilização dos últimos 30 (trinta) dias:
- Status de trabalhos bem-sucedidos, trabalhos com falha e trabalhos com erros;
- Máquinas protegidas e máquinas replicadas;
- Status do repositório, contendo volume consumido e volume livre;

Acordo de Nível de Serviço (ANS):

- Os tempos máximos de atendimento especificados nas tabelas a seguir, sob pena de multa;
- Em casos emergenciais, quando houver a paralisação nas atividades do negócio ou uma demanda de nível superior, a CONTRATANTE poderá abrir chamados emergenciais, com o ANS diferenciado, cujo tempo de resposta para todas as atividades listadas na tabela abaixo passam a ter tempo máximo de resposta de 60 minutos. A CONTRATANTE deverá designar até 4 (quatro) pessoas que poderão abrir chamados emergenciais.

Chamados de Firewall:

Atividade	Tempo de Resposta Máximo
Alteração e inclusão de regras.	8 horas após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Alteração de configurações.	8 horas após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Atualização (implementação de patches e fixes).	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pela CONTRATANTE.
Início de atuação remota para resolução de problemas.	4 horas após abertura de chamado
Implementação de novos serviços ou dispositivos.	48 horas após abertura de chamado
ANS para serviços de Firewall	

Chamados de Backup Profissional:

Atividade	Tempo de Resposta Máximo
Proteção de um novo servidor/computador.	48 horas após abertura de chamado.
Alteração das políticas atuais de backup.	8 horas após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Atualização (implementação de patches e fixes).	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pela CONTRATANTE.
Início de atuação remota para resolução de problemas.	4 horas após abertura de chamado.
Recuperação de dados e/ou servidor/computador por completo.	3 horas após abertura de chamado, exceto quando for necessária uma janela de manutenção.
ANS para serviços de Backup	

Requisitos de Capacitação

4.2. Será necessário treinamento à equipe que atuará com a solução. O repasse de conhecimento deverá ocorrer de acordo com as necessidades e conveniência do contratante, podendo envolver treinamentos presenciais ou remotos, disponibilização de manuais, orientações práticas e acompanhamento técnico durante a fase de implantação e pós-implantação.

Requisitos Legais

4.3. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção

4.4. Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativa e evolutiva pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

Segue em tópicos diversos do Item 4 deste Termo de Referência os requisitos necessários para manutenção de cada objeto.

Requisitos Temporais

4.5. Os serviços devem ser prestados no prazo máximo de 30 (trinta) dias corridos para a capital do estado do Tocantins e de 30 (trinta) dias corridos para as demais localidades, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.6. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.7. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

4.8. Na execução dos serviços, deverão ser observados os seguintes prazos:

Atividade, Tarefa ou Serviço	Prazo máximo de início de atendimento	Prazo máximo de solução de problema
Planejamento	2 dias	15 dias
Implantação	2 dias	30 dias
Testes e Homologação	2 dias	15 dias
Operação Assistida	2 dias	30 dias

4.8.1 Os serviços serão prestados no âmbito do CRM-TO, nas cidades/endereços descritos abaixo:

● Palmas – TO

- Sede Provisória: ACSV 71 (704 Sul), Av. LO 15, Lote 18, 1º Piso, Plano Diretor Sul, Palmas/TO, CEP: 77022-322.
- Sede Principal: Quadra ACSU SE 70 CONJ. 01, Lote 01, Plano Diretor Sul, Palmas/TO, CEP 77022-306.

Durante a vigência do contrato, os custos inerentes à migração dos serviços e equipamentos, objeto desse contrato, da Sede Provisória de Palmas para a Sede Principal, em virtude da mudança de instalações físicas da CONTRATANTE, deverão ser integralmente considerados e inclusos no valor global da proposta da CONTRATADA.

Requisitos de Segurança e Privacidade

4.9. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, Política de Segurança de Rede, Políticas de segurança para dispositivos móveis, Políticas de privacidade de dados online – LGPD, ISO/IEC 27001, Framework de Cibersegurança do NIST.

Requisitos Sociais, Ambientais e Culturais

4.10. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

- Acessibilidade digital, Ética na IA e nos dados, Combate à desinformação, Inclusão social, Segurança e bem-estar online, Uso de energia renovável, Gestão de lixo eletrônico,

Requisitos da Arquitetura Tecnológica

4.11. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.12. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

Requisitos de Projeto e de Implementação

Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos no Item 4 deste Termo de Referência.

Requisitos de Implantação

4.13. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos no Item 4 deste Termo de Referência.

Requisitos de Garantia e Manutenção

4.14. O prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e suas atualizações.

Requisitos de Experiência Profissional

4.15. Os serviços de assistência técnica, suporte, garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

Requisitos de Formação da Equipe

4.16. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:

- **Formação Acadêmica:** Nível superior completo ou técnico em Tecnologia da Informação, Ciência da Computação, Engenharia de Redes, Segurança da Informação ou áreas correlatas.
- **Experiência Profissional Comprovada:** Mínimo de 1 (ano) anos de experiência comprovada na área de segurança da informação ou infraestrutura de rede, com atuação direta em implantação, gerenciamento e suporte de soluções de segurança, incluindo Firewall (NGFW) e Backup Corporativo.
- **Certificações Técnicas Relevantes:** Possuir, no mínimo, 1 (uma) certificação ativa de fabricante ou de órgão certificador reconhecido em cada uma das seguintes áreas, ou uma certificação equivalente que abranja múltiplos domínios: Segurança de Rede, Backup, Recuperação de Desastres e Segurança de Endpoints.
- **Habilidades de Suporte e Comunicação:** Capacidade comprovada de realizar atendimento técnico (remoto e presencial), registrar, acompanhar e solucionar chamados técnicos, elaborar documentação ("As Built"), transferir conhecimento e se comunicar de forma clara e eficaz com a equipe do Contratante.

- **Disponibilidade:** Flexibilidade para atuar em regime de suporte técnico integral (24/7), conforme a natureza continuada e crítica dos serviços gerenciados.

Requisitos de Metodologia de Trabalho

- 4.17. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.
- 4.18. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.
- 4.19. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana de maneira eletrônica e 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana por via telefônica.
- 4.20. A execução do serviço deve ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

ESPECIFICAÇÕES TÉCNICAS DETALHADAS DE CADA SOLUÇÃO QUE COMPREENDE OS SERVIÇOS GERENCIADOS

- 4.21. Todos os equipamentos, produtos, peças ou softwares ofertados para a composição dos serviços gerenciados solicitados deverão ser novos, de primeiro uso e não constarem, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante. Ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou ciclo de vida, devendo estar em linha de produção e cobertos por suporte e garantia do fabricante, bem como possuir todo o licenciamento necessário para o funcionamento dos recursos exigidos neste Termo de Referência, pelo período mínimo de 12 (doze) meses.
- 4.22. Todos os softwares deverão ser fornecidos em sua versão mais atual do fabricante, devendo constar na proposta comercial o seu PART NUMBER e/ou versão para efeito de comprovação, bem como seu quantitativo;
- 4.23. É obrigatório o atendimento técnico de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor. Para tanto, o fornecedor deve disponibilizar documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante para análise da equipe técnica da contratante.
- 4.24. O simples fato de “COPIAR” e “COLAR” o descritivo contido no edital não será caracterizado como descritivo da proposta;
- 4.25. Serão aceitos como documentos de comprovações técnicas:
- Documentos emitidos pelo fabricante dos produtos, na língua portuguesa ou inglesa, de preferência disponíveis na Internet (indicar o link onde podem ser obtidos). Declarações do fabricante somente serão aceitas se utilizadas em conjunto com documentos de comprovação como manuais, páginas da Internet, telas do produto ou outros documentos técnicos, que contenham o requisito solicitado;
 - Declarações de conformidade com o termo, no caso do item de comprovação referir-se apenas a serviço a ser prestado pelo proponente;

LOTE ÚNICO: ITEM 1 - SERVIÇOS TÉCNICOS ESPECIALIZADOS DE IMPLANTAÇÃO

- Este item descreve os serviços técnicos especializados destinados à implantação das soluções que compõem cada um dos serviços gerenciados, sendo: Firewall e Backup;
- A CONTRATANTE solicitará as implantações dos serviços adjudicados por meio de OS - Ordem de Serviço com o nome dos serviços a serem implantados, de acordo com as horas contidas no tópico “Consumo de Horas de Implantação por Serviço/Solução”;
- O prazo máximo para implantação pela CONTRATADA será de 30 (trinta) dias corridos, contados a partir da emissão da Ordem de Serviço;
- Caberá a CONTRATANTE subsidiar toda infraestrutura necessária para implementação das soluções que compõem cada serviço, exemplo: locais de instalação dos appliances de Firewalls (Racks, gavetas).
- Todos os serviços de instalação deverão ser realizados com transferência de conhecimento aos servidores da CONTRATANTE, sem ônus;
- As fases da implantação dos serviços devem contemplar:
 - Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento da solução a ser implementada, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano testes, bem como quaisquer outros itens que sejam necessários para a implantação da respectiva solução. Deve-se considerar as janelas de manutenção da CONTRATANTE, plano de rollback e o escopo definido. Os responsáveis técnicos da CONTRATANTE acompanharão e aprovarão o planejamento;
 - Implementação: após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento dos prazos pactuados e o foco principal do projeto visando tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.
 - Etapa de Testes: todos os controles implantados para a ativação dos serviços gerenciados de segurança deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço;
 - Homologação: Após a conclusão dos testes, a solução deverá ser formalmente homologada pela CONTRATANTE, com a finalidade de iniciar a monitoração, operação dos serviços e gerenciamento do ambiente, dentro dos níveis de serviço acordados;
- A CONTRATANTE terá o prazo de 7 (sete) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração dos serviços contratados, para emitir o relatório de homologação (aceite);
- O serviço será aceito se, e somente se, houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos utilizados, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações, comparadas aos itens deste Termo;
- Ao término de cada implementação, a CONTRATADA deverá entregar Caderno de Documentação “As Built” da solução implementada, no qual conste todos os detalhes da instalação, configuração, testes, procedimentos de contingência bem como histórico de todo esse processo;
- Consumo de Horas de Implantação por Serviço/Solução:
 - Serão adquiridas as horas necessárias para a implantação, de acordo com a solicitação da CONTRATANTE, a partir de um total de 36h (trinta e seis horas) que contempla a implementação de todas as soluções/serviços contidas neste certame;
 - Para efeitos de formulação da proposta comercial, deverão ser considerados o quantitativo de horas unitárias de implantação da tabela abaixo para cada tipo de Serviço/Solução:

ITEM	DESCRIÇÃO	HORAS UNIT.
1	Implantação de 1 (um) appliance de Firewall	24
2	Implantação de 1 (uma) instância de Backup	3

Consumo de horas Solução/Serviço

○ Escopo dos Serviços de Implantação de Firewalls:

- Instalação das Soluções de Firewalls, conforme contratado;
- Configurar as Soluções de Firewall conforme segmentação de rede definida pela CONTRATANTE;
- Atualização e aplicação de correções nas soluções de Firewall;
- Implementação/migração de regras de Filtragem;
- Implementação/migração de regras de NAT;
- Implementação/migração de regras de QoS;
- Implementação/migração de regras de Filtro de Conteúdo Web, IPS, Anti-malware, Controle de Aplicativos, e Proteção Contra Ameaças Avançadas;
- Integração com o Active Directory;
- Tuning de configuração e regras de filtragem, removendo as regras inalcançáveis, adicionando uma descrição para cada regra implementada, remoção de elementos de rede não utilizados;
- Testes gerais, validando o funcionamento das aplicações após a implementação dos Firewalls;

○ Escopo dos Serviços de Implantação da Solução de Backup:

- Instalar e configurar o software/agente de backup nos servidores a serem protegidos;
- Configurar políticas backup e de retenção de dados relacionada ao ambiente protegido;
- Configurar replicação do Backup Principal para unidade de Backup Secundária, se necessário;
- Executar testes de backup e restore;

LOTE ÚNICO: ITEM 2 - SOLUÇÃO DE FIREWALL

● Características específicas de performance e hardware.

- Deverá ser fornecido 1 (um) appliance de firewall (NGFW) destinado à proteção do ambiente, com licenciamento vigente por 12 (doze) meses, contemplando IPS, proteção antimalware avançada, sandbox, controle de aplicações, filtragem de conteúdo, serviço antispam, gerenciamento, relatórios e suporte técnico.
- Desempenho em modo Threat Protection (IPS, antimalware e controle de aplicações habilitados) mínimo de 600 (seiscentos) Mbps;
- Desempenho em modo de Inspeção (descriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 250 (trezentos) Mbps;
- Desempenho de IPS (Intrusion Prevention System), mínimo de 900 (novecentos) Mbps;
- Deve suportar, no mínimo, 700 (setecentos) Mbps de desempenho de VPN IPSEC;
- Suporte mínimo de 600.000 (seiscentos mil) conexões simultâneas/concorrentes;
- Suporte mínimo de 5.000 (cinco mil) novas conexões por segundo;
- Interfaces Ethernet: mínimo de 5 (cinco) portas 1GbE RJ-45;

- Deve suportar expansão futura de armazenamento para no mínimo 120 (cento e vinte) GB ou armazenamento na nuvem do fornecedor;
- Interface de console: mínimo de 1 (uma) (RJ-45 ou equivalente).;
- Deve possuir no mínimo 1 (uma) interface USB 3.0;
- Deve suportar VPN IPsec Client-to-Site para no mínimo 50(cinquenta) usuários simultâneos;
- Deve suportar VPN SSL Client-to-Site para no mínimo 40 (quarenta) usuários simultâneos e caso necessitar de licença adicional, deve estar licenciada para, no mínimo, 10 (dez) usuários simultâneos;
- Deve suportar no mínimo 50 (cinquenta) túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos, já licenciados;

● Características Gerais:

- Devem ser fornecidas todas as licenças necessárias para o funcionamento das funcionalidades de proteção, gerenciamento e relatórios aqui exigidos pelo período mínimo de 12 (doze) meses;
- O equipamento ofertado deverá pertencer à atual (mais recente) ou à penúltima geração de hardware disponibilizada pelo fabricante. Não serão aceitas versões anteriores a estas, mesmo que ainda comercializadas ou em linha de produção;
- A solução deverá ser fornecida por um único fabricante, com funcionalidades integradas e gerenciadas em uma única console, local ou centralizada (on-premises e/ou em nuvem/Data Center do fornecedor);
- A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL;
- Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço;
- O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, de um NGFW, Appliance dedicado de segurança não sendo baseado em plataforma X86 ou equivalente;
- A solução ofertada deverá ser homologada pela ANATEL;
- Não serão aceitos Sistemas Operacionais do Tipo “Harderizado”, SO dedicado/integrado de segurança;
- Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;
- Por funcionalidades de NGFW entende-se: NGFW com AppID, IPS/AV, URL, integração a usuários e controle granular;
- Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP;
- O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL/TSL onde o mesmo deverá ser descriptografado de forma transparente a aplicação, possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante, verificado possíveis ameaças e então re-criptografado e enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades. O recurso poderá ser fornecido através de uma licença adicional ao equipamento;

- Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a TLS 1.3;
- Deve implementar mecanismo de sincronismo de horário através do protocolo NTP, e permitir a configuração do tempo do intervalo de pesquisa;
- Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware e IPS por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.
- Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de IPS, Gateway Antivirus/Anti-Spyware;
- Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;
- Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN;
- Deve suportar DHCP relay;

● Características Anti-Malware:

- Deve possuir módulo de Anti-Vírus integrado ao próprio appliance de segurança;
- A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;
- Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, FTP, e TCP Stream;
- Permitir o bloqueio de malwares (vírus, worms, spyware e etc);
- A solução deverá receber atualizações de um serviço baseado em cloud;

● Filtro de Conteúdo Web:

- Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 70 (setenta) categorias distintas, com mecanismo de atualização e consulta automáticas;
- Permitir a customização de página de bloqueio;
- Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;
- Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana;

● Controle de aplicações:

- Reconhecer no mínimo aplicações como: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;
- Possibilitar o controle sobre aplicações de forma granular;
- Devem ser aplicados por usuário e por grupo;
- Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, dia, dias da semana, mês e ano que a ação deverá ser tomada;
- Controlar o uso dos serviços de Instant Messengers, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

● **Proteção Contra Ameaças Avançadas:**

- A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída;
- A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída;
- A solução deverá possibilitar a implementação de políticas de inspeção, decodificação e recriação de tráfego, bem como o monitoramento de diferentes tipos de protocolos e fluxos de dados, de acordo com as necessidades e políticas de segurança definidas pela CONTRATANTE.
- A solução deverá identificar e bloquear comunicações com infraestruturas maliciosas, utilizando feeds de reputação e listas continuamente atualizadas em nuvem;
- Implementar detecção e bloqueio imediato de malwares, sendo que a solução deve inspecionar arquivos com no mínimo 10Mb;
- Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;
- A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliances através de assinaturas;
- Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;
- Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
- Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real;
- Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .pdf, .zip, .rar) e Android APKs no ambiente controlado;
- A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo;

● **Características de VPN:**

- Suportar algoritmos Hash no mínimo SHA-256, SHA-384 e SHA-512;
- Suporte a Diffie-Hellman: Grupos 1, 2, 5 e 14;
- Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2;
- Autenticação via de túneis IPsec via certificado digital para VPNs Site-to-Site e Client-to-Site;
- A solução ofertada deve possuir suporte a VPN Client-to-Site, com pleno suporte aos modos SSL VPN e IPsec VPN, em suas versões de firmware mais recentes.
- Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;
- Permitir a redundância para terminação de VPN no caso de queda do circuito primário;
- Interoperabilidade baseada em padrões abertos (IPsec/SSL), independentemente do fabricante remoto;
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
-

● **Características de NAT:**

- Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores

internos com endereços reservados sejam acessados externamente através de endereços válidos;

- Possuir mecanismo que permita conversão de portas (PAT);
- Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many e many-to-one;

● Características de QoS:

- Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida para cada regra definida;
- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade;
- Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);
- Permitir remarcação de pacotes utilizando TOS e/ou DSCP;
- Limitar individualmente a banda utilizada por aplicação;
- Deverá controlar (limitar) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá controlar (limitar) individualmente a banda utilizada por subrede de origem e destino;
- Deverá controlar (limitar) individualmente a banda utilizada por endereço IP de origem e destino;

● Características de Roteamento:

- Suportar os protocolos de roteamento RIP, OSPF e BGP
- Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;
- Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação;
- O equipamento deve possuir suporte a roteamento IPv4 e IPv6;
- O equipamento deve suportar roteamento baseado em aplicativo permitindo a criação de regras de encaminhamento baseadas na identificação do aplicativo em uso;
- A solução ofertada deve possuir suporte a roteamento TOS (Type of Service), permitindo a definição de múltiplas rotas de política utilizando os mesmos parâmetros de IP de origem, IP de destino e valores de serviço.

● Características de SD-WAN:

- A solução deverá implementar tecnologia de SD-WAN (Software Defined WAN);
- Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos: Latência, Jitter e Perda de pacotes;
- A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;

● Características de Gerenciamento Nativo:

- Fornecer gerência remota, com interface gráfica WEB segura nativa, utilizando o protocolo HTTPS;
- Possuir interface CLI (orientada a linha de comando) segura para a administração do firewall a partir do console com conexão via protocolo SSH;
- Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição

de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração;

- Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica;
- Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração;
- Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;
- Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW;
- Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados;
- Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps e ameaças identificadas;
- Permitir, através da interface gráfica a visualização em forma gráfica e em tempo real das estatísticas do uso de processamento e tráfego de rede em todas as interfaces do NGFW;
- Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças.
- Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreo das configurações aplicadas no produto;
- Ser capaz de implementar a funcionalidade de “Zero-Touch”, permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada;
- A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android;
- O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB;
- O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW;

● Autenticação:

- Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+ e Single Sign On;
- Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;
- O appliance de firewall deve suportar base de usuários interno

● Gerenciamento Centralizado e Relatórios Analíticos:

- Em conjunto com os firewalls, a contratada deverá fornecer uma solução de gerenciamento centralizado, hospedada on-premises, na nuvem do fornecedor ou do mesmo fabricante dos appliances de firewall ofertados, destinada à administração e à geração de relatórios completos de todos os equipamentos de segurança contemplados neste certame.
- A plataforma deverá estar hospedada em ambiente de nuvem, sob responsabilidade do fabricante, garantindo alta disponibilidade, redundância e escalabilidade.
- Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções dos usuários da console que

determinem usuários:

- Grupos de firewalls;
- Funcionalidades permitidas por firewall ou grupo de firewalls de acordo com o perfil de uso designado;
- Perfil de nível de acesso (escrita, leitura, administração);
- Deve suportar organizar os dispositivos administrados em grupos. Estes grupos devem permitir isolamento tanto de acesso para os administradores como de configuração massiva ou individual;
- Deve apresentar estado dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;
- Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
- O gerenciamento deve permitir/possuir:
 - Criação e administração de políticas de firewall;
 - Monitoração de logs;
 - Investigação de eventos de segurança;
 - Acesso concorrente de administradores, conforme políticas e perfis previamente definidos ;
- Deve permitir o provisionamento e configuração sem intervenção de operadores (Zero-Touch). Os firewalls devem se conectar automaticamente à plataforma de gerência, e à partir desta conexão receberem as configurações previamente determinadas pelos operadores da plataforma;
- A solução de gerenciamento deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL;
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados;
- A solução deve possuir tela situacional com todo os inventários de firewalls gerenciados centralizadamente, informando no mínimo para o administrador:
 - Nome do firewall;
 - Número de série;
 - Modelo;
 - Versão do firmware e estado da conectividade do equipamento com a gerência em online ou offline;
- Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez;
- A solução deve possuir Dashboard com sumario de alertas e informação de status de licença;
- A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo;
- A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão na console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN;
- A solução deve permitir a criação de modelos de configuração (templates) para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls;
- A solução deve possibilitar a geração de templates de configuração à partir da configuração vigente em um firewall selecionado pelo administrador da plataforma, e possibilitar que este template possa ser editado e utilizado em outros firewalls gerenciados pela plataforma;
- Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas;

- Deve incluir console de configuração e monitoramento SD-WAN, possibilitar a criação de políticas SD-WAN em todos os elementos gerenciados, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall;
- Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente;
- Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, este processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente;
- A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada ;
- A solução deve oferecer monitor de auditoria de configurações aplicadas aos firewalls gerenciados pela plataforma, permitindo comparativo diferencial entre registros para rápida identificação de configurações e alterações aplicadas;
- A solução deve oferecer módulo centralizado que possibilite realização e armazenamento de backup de configurações dos firewalls gerenciados;
- A solução deve possibilitar o monitoramento em tempo real dos firewalls gerenciados, informando minimamente:
 - Utilização de CPU/Processamento;
 - Aplicações em uso e seu consumo de banda;
 - Interfaces em uso e utilização de banda;
 - Conexões concorrentes em uso;
- A solução deverá prover relatórios avançados/analíticos com no mínimo histórico de 90 dias;
- A solução deverá prover relatórios referente as atividades dos usuários;
- A solução deverá prover relatórios referente ao uso de aplicações, com no mínimo as seguintes informações:
 - Nome da aplicação;
 - Percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados;
- A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:
 - Nome do usuário;
 - Percentual que tráfego do usuário representa na rede;
 - Quantidade de Megabytes trafegados;
- A solução deverá permitir geração e envio agendado de relatórios;
- A solução deve permitir a customização de alertas e notificações, possibilitando o envio de e-mail com as informações relativas a este evento;
- A solução deve possibilitar configuração e monitoramento centralizados de VPNs entre os firewalls gerenciados;
- A solução deve apresentar consoles de indicação dos principais usuários contendo:
 - Usuários utilizando mais conexões;
 - Usuários consumindo mais dados;
- A solução deve apresentar console de indicação de:
 - Virus/Spyware bloqueados;
 - Intrusões bloqueadas;
 - Botnets bloqueados;

- A solução deve apresentar console de monitoramento de produtividade dos usuários, indicando suas características de navegação de acordo com políticas previamente estabelecidas e categorizadas como:
 - Produtivas;
 - Não produtivas;
 - Aceitáveis para a política de uso corporativa;
 - Inaceitáveis para a política de uso corporativa;
 - Customizadas;
- Qualificações:
 - O Fabricante da solução de firewall deve comprovar participação no MAPP (Microsoft Active Protections Program);
 - Visando estabelecer efetividade de segurança dos firewalls e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá possuir tecnologia ou equipamento avaliada e certificada pelo NetSecOPEN.
 - O fabricante da solução deve ser citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes;

LOTE ÚNICO: ITEM 3 - SOLUÇÃO DE BACKUP

● Características Gerais

- Cada unidade deste item representa a proteção de uma instância de servidor, incluindo a licença do software de backup, bem como os serviços necessários para o monitoramento, gerenciamento e suporte do backup. A contratação da solução de backup/restore será realizada de forma unitária, ou seja, considerando a quantidade de instâncias protegidas, independentemente da volumetria do ambiente virtual ou do número de processadores envolvidos.
- Para a área de armazenamento necessária para o repositório do backup, será realizado a contratação do item (SERVIÇOS DE ARMAZENAMENTO)
- Realizar via solução profissional de backup especificada abaixo a proteção (backup) completa (sistema operacional, aplicativos instalados, configurações e dados), diário e/ou intervalos pré-determinados, automaticamente, dos servidores críticos elencados pela contratante;
- A licença estará em uso apenas enquanto estiver executando a rotina de backup referente ao objeto protegido, isto é, máquina virtual, servidor físico ou banco de dados. Se o objeto for desassociado da política de execução de backup, a licença estará livre para uso em outro objeto protegido. Portanto, os dados de backup dos objetos antigos e novos deverão permanecer disponíveis para restauração até o término de suas respectivas políticas de retenção;
- A solução ofertada deverá ser compatível nativamente com os seguintes hipervisores:
 - VMware ESXi;
 - Microsoft Hyper-V;
- A solução ofertada deverá possuir compatibilidade conforme as especificações abaixo:
 - VMware vCenter e vSphere ESXi versões 7 e superiores;
 - Nuvem Amazon Web Services (AWS) EC2 e Microsoft Azure VM;
 - Microsoft Active Directory 2012 e superiores;
 - Microsoft SQL Server 2012 SP4 e superiores;
 - Oracle Database 12c Release 2 e superiores;
 - MySQL 9 ou superiores;
 - PostgreSQL 13 ou superiores;

- Suportar, nos clientes de backup, os sistemas operacionais:
 - Microsoft Windows Server 2012 e superiores;
 - Microsoft Windows 10 e superiores;
 - CentOS Linux 7 e superiores;
 - Debian Linux 10 e superiores;
 - Oracle Linux 7 e superiores;
 - Ubuntu 18.04 LTS e versões LTS superiores;
- Suportar, nos clientes para backup, no mínimo os sistemas de arquivos do tipo: ext3, ext4, XFS, FAT32, NTFS e ReFS;
- Possuir recurso para possibilitar a reconstrução do catálogo dos dados de backup armazenados em disco e fita;
- Possuir catálogo que centraliza as informações de gerenciamento do software de backup incluindo:
 - Objetos protegidos;
 - Rotinas de backup e políticas de retenção;
 - Fitas e seu conteúdo;
 - Fitas com cópias em cofres externos e demais informações de gerenciamento;
- Suportar deduplicação a nível de blocos e em volumes e compartilhamentos de rede apresentados através de DAS (Direct Attached Storage), SAN (Storage Area Network) e NAS (Network Attached Storage);
- Suportar deduplicação de dados na origem (source deduplication), de forma que sejam enviados apenas novos blocos de dados criados e/ou modificados a partir do último backup;
- Possuir criptografia de dados na origem (direto no cliente ou servidor de proxy de backup), de uma forma que seja garantido que o dado trafegará criptografado na LAN (Local Area Network) ou WAN (Wide Area Network);
- Possuir módulo nativo de criptografia AES (Advanced Encryption Standard) 256 bits;
- Suportar qualquer tecnologia utilizada na infraestrutura de armazenamento como destino do backup: DAS, NAS e SAN, sem prejuízos das demais funcionalidades suportadas pelo software;
- Paralelizar a gravação de dados de uma rotina de backup em diferentes caminhos pertencentes à vários dispositivos de armazenamento;
- Permitir a gravação serial e simultânea de várias rotinas de backup, provenientes de clientes distintos, em um único caminho pertencente à um dispositivo de armazenamento (funcionalidade conhecida como multiplexação);
- Permitir exportar o conteúdo de backup para mídia removível, possibilitando o transporte físico de dados até o destino;
- Ser flexível e escalável, permitindo sua instalação, configuração e uso em sites remotos interligados ao site principal através da WAN ou através de LAN;
- Permitir replicação de uma origem para múltiplos destinos;
- Suportar a replicação do backup para diversos sites remotos, permitindo ainda que a restauração dos dados seja feita através das cópias armazenadas remotamente;
- Permitir replicação e consolidação de dados de múltiplas origens para um destino central;
- Prover recursos de deduplicação e compressão tanto no site principal como nos sites remotos;
- Possuir interface gráfica e/ou web, capaz de gerenciar um ou mais sites de forma centralizada;
- Suportar o armazenamento local de dados;
- Suportar deduplicação de blocos localmente, de forma que o cliente ou servidor de proxy envie, em LAN e WAN, apenas os blocos de dados modificados para o site principal;

- Suportar o envio do backup para unidades de fita LTO Ultrium 8 e superiores;
- Deverá permitir cópias adicionais do backup principal com funcionalidade de criar múltiplas cópias em fitas;
- Suportar a gravação em fitas WORM (Write Once Read Many);
- Suportar a gravação em bibliotecas de fitas automatizadas;
- Possibilitar o backup e a restauração das informações em disco e fita;
- Suportar as operações de backup e restauração em paralelo;
- Permitir localizar e restaurar um arquivo, via pesquisa por nome do mesmo no catálogo da ferramenta;
- Possuir a capacidade de efetuar backup para disco e fita com retenções, através de políticas pré-definidas e agendadas;
- Possuir a função de disk staging, para gravação de dados em disco e, posteriormente, a cópia para outro tipo de mídia (disco e fita);
- Possuir a funcionalidade de criar múltiplas cópias de backups armazenados, com a opção de recuperação dos dados através da cópia secundária se a cópia primária não estiver mais disponível;
- Permitir a criação de imagens de servidores físicos Linux e Windows para recuperação de desastres de forma nativa e sem a utilização de software de terceiros (bare-metal restore);
- Permitir os backups e restore do "system state" do Windows de forma nativa e sem a utilização de software de terceiros;
- Deverá permitir a verificação de vírus durante a restauração de máquinas virtuais, abortando a recuperação ao detectar aplicações maliciosas;
- Suportar realizar os backups de maneira incremental, com apenas um backup full e todos os demais incrementais até o término do período de retenção;
- Gerar logs com as informações: o que foi restaurado, quem restaurou e para onde foi restaurado;
- Permitir a integração com o Microsoft SQL Server;
- Executar backup de bases de dados do SQL Server de forma "online", ou seja, sem a parada do banco;
- Executar backup de logs transacionais, possibilitando a criação de rotina de backup;
- Permitir a integração com Microsoft Active Directory;
- Permitir a integração com Oracle Database, realizando o backup de forma "online" via Oracle RMAN;
- Permitir exportar uma base de dados Oracle diretamente a partir do arquivo de backup;
- Permitir integração com PostgreSQL, executando o backup de bases de dados do PostgreSQL de forma "online", ou seja, sem a parada do banco e de forma consistente;
- Permitir integração com MySQL, executando o backup de bases de dados do MySQL de forma "online", ou seja, sem a parada do banco e de forma consistente;
- Permitir a recuperação de uma máquina/servidor físico instantaneamente no ambiente virtual VMware vSphere ou Microsoft Hyper-V, com inicialização rápida, a partir de seus arquivos de backup, sem a necessidade de esperar o término do processo de restauração;
- Permitir adicionar automaticamente as máquinas virtuais descobertas em rotinas de backup pré-definidas, baseado no domínio de proteção que estão contidas;
- Permitir a restauração granular a nível de arquivos das máquinas virtuais protegidas, sem a necessidade de se restaurar a máquina virtual inteira;
- Deverá ter a capacidade de testar a consistência do backup, emitindo relatório de auditoria para garantir a capacidade de recuperação;
- Deverá suportar a replicação remota a fim de replicar os dados das máquinas virtuais entre soluções de armazenamento distintas, inclusive de diferentes fabricantes;
- Possuir módulo de gerenciamento central com interface gráfica (ou web) responsável

pela administração de todas as operações de backup, configurações, gerenciamento, monitoração, criação/atualização de políticas do ambiente e rotinas associadas à proteção de dados de todos os sites;

- A solução de software de backup não deve ser operada exclusivamente por linhas de comando - CLI;
- Possuir gerenciamento das operações da infraestrutura de backup em modo gráfico, que permita o monitoramento em tempo real das rotinas de backup e status dos dispositivos e clientes de todo o ambiente;
- Prover monitoramento, através de interface gráfica ou web, em tempo real, das rotinas de backup sendo executados;
- Possuir recursos avançados de agendamento de rotinas de backup, para datas específicas, dias da semana recorrentes, dia do mês recorrente. Primeiro, segundo terceiro e último dia do mês;
- Possuir agendamento de rotinas de backup, sem a utilização de utilitários de agendamento de servidores. O agendamento deve ser controlado pelo gerenciador de backup;
- Possuir mecanismo de auditoria para o controle de acesso, em operações realizadas através de interface gráfica ou web e linha de comando (interface CLI), contendo no mínimo, as seguintes informações: data e hora da operação, usuário que realizou a operação, operação realizada;
- Permitir o envio automático de alertas por e-mail e SNMP (Simple Network Management Protocol) através de traps ou consultas, com o objetivo de reportar eventos ocorridos nas operações do software de backup;
- A solução deve oferecer notificações sobre problemas, bem como sobre realização de backups, por meio de logs, e-mail ou mensagens na console;
- A solução deverá permitir a visualização em sua console gráfica ou geração de relatórios de backup, os quais permitam obter minimamente as seguintes informações:
 - Horário de início e término de uma rotina de backup;
 - Tempo de duração de uma rotina de backup;
 - Status do backup (situação);
 - Relação dos objetos incluídos na rotina de backup;
 - Volume de dados na origem durante a rotina de backup;
 - Volume de dados com compressão e deduplicação;
 - Taxa de deduplicação de dados;
 - Suportar a geração de relatórios sobre o consumo de licenças;
- Suportar a geração de relatórios de máquinas virtuais protegidas, contendo:
 - Quantidade total de máquinas virtuais na infraestrutura virtual;
 - Relação das máquinas virtuais, informando que possuem backup e quais não estão backupeadas;
 - Quantidade de versões de backup armazenadas no repositório de backup para cada máquina virtual;
 - Nome do cluster virtual que a máquina virtual se encontra;
 - Data da última execução da rotina de backup com sucesso;
 - Repositório no qual o backup do objeto está armazenado;
- Suporte do software
 - Deverá ser fornecido suporte técnico do FABRICANTE por 12 (doze) meses, com atendimento 24/7;
 - O fabricante deverá oferecer canais de comunicação e ferramentas adicionais de suporte online como página de suporte técnico na Internet com disponibilidade de atualizações das versões dos softwares;
 - Durante o período de suporte, deverão ser fornecidas todas as atualizações de

versões do produto, bem como correções e patches, sem custo;

LOTE ÚNICO: ITEM 4 - SERVIÇOS DE ARMAZENAMENTO PARA BACKUP (TB)

● Características Gerais

- Deve ser fornecido recursos em bloco HDD (Hard Disk Drive) de armazenamento baseado em discos do tipo rígido, possibilitando a alocação dos mesmos para armazenamento de dados.
- Cada unidade deste item representa 1 TB (terabyte), sendo permitido à CONTRATADA contratar a quantidade necessária de unidades em TB a serem entregues pela CONTRATANTE, garantindo o armazenamento adequado dos backups e a proteção dos dados institucionais.

Requisitos de Segurança da Informação e Privacidade

4.26. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.26.1 LGPD (Lei Geral de Proteção de Dados);

4.26.2 ABNT NBR ISO/IEC 27001 – SGSI;

4.26.3 ABNT NBR ISO/IEC 27002;

4.26.4 Privacidade por padrão e desde a concepção (Privacy by Default and Design)

Vistoria

4.27. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 8 horas às 14 horas.

4.28. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.29. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.30. Caso o interessado opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

4.31. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o Contratado assumir os ônus dos serviços decorrentes.

Sustentabilidade

4.32. O Contratado deverá seguir todos os critérios de sustentabilidade inseridos no Guia Nacional de Contratações Sustentáveis.

Indicação de marcas ou modelos

4.33. Na presente contratação não será admitida a indicação de marca(s), característica(s) ou modelo(s).

Subcontratação

4.34. Não será admitida a subcontratação do objeto contratual.

Da exigência de amostra

4.35. Na contratação pretendida não serão exigidas amostras

Garantia da contratação

4.36. Não haverá exigência da garantia da contratação dos art. 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

Informações relevantes para o [dimensionamento E/OU apresentação] da proposta

4.37. Nas propostas de preços para a licitação por preço global, cada serviço ou produto do lote deverá estar discriminado em itens separados, de modo a permitir a identificação do seu preço individual na composição do preço global, para fins de aplicação do disposto no § 4º do art. 12 da Instrução Normativa SGD/ME nº 94, de 2022, e no art. 26 da Lei nº 14.133, de 2021.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

- nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;
- prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

- indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;
- atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
- vedado à CONTRATADA manter vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, devendo essa proibição constar expressamente nas declarações de contratação.

- propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
- fazer a transição contratual, quando for o caso.

5.3. São obrigações do órgão gerenciador do registro de preços:

- efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
 - as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
 - definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;
- definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:
 - a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
 - as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e
 - as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1 Início da execução do objeto: 30 dias da assinatura do contrato.

6.1.2 Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho: A descrição detalhada encontra-se discriminada no Estudo Técnico Preliminar;

Local e horário da prestação dos serviços

6.2. Os serviços serão prestados conforme descrito no Item 4.8.1 deste Termo de Referência

6.3. Os serviços serão prestados descrito no Item 4.8.1 deste Termo de Referência

Rotinas a serem cumpridas

- A execução contratual observará as rotinas detalhadas no Estudo Técnico Preliminar;

Materiais a serem disponibilizados

6.4. Para a perfeita execução dos serviços, o Contratado deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

6.4.1 1. Todos os equipamentos de hardware e softwares/licenças necessários para a plena execução dos serviços de implantação e gerenciamento, conforme especificações técnicas do Anexo I, em regime de comodato, sem ônus adicional para a Contratante;

6.4.2 2. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades solicitadas pelo contratante e qualidades estabelecidas no Estudo Técnico Preliminar, promovendo sua substituição quando necessário.

Informações relevantes para o dimensionamento da proposta

6.5. A demanda do órgão tem como base as seguintes características:

6.5.1 Ambiente de Rede e Usuários:

6.5.1.1. Estimativa de 4 (quatro) servidores (físicos e virtuais) a serem cobertos pelos serviços de Backup;

6.5.1.2. Estimativa de 6 TB (terabytes) de capacidade inicial para armazenamento de backup;

6.5.1.3. Necessidade de um appliance de Firewall na borda da rede.

6.5.2 Formas de transferência de conhecimento

6.6. A transferência do conhecimento deverá ser realizada observando-se o que segue:

6.6.1 A transferência de conhecimento aos servidores da CONTRATANTE deverá ser realizada durante todos os serviços de instalação, sem qualquer ônus.

6.6.2 A transferência de conhecimento ocorrerá durante a etapa de "Operação Assistida", que consiste no acompanhamento contínuo do ambiente em produção e suporte ativo.

Procedimentos de transição e finalização do contrato

6.7. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.7.1 A CONTRATADA deverá realizar a transição contratual, assegurando a transferência de conhecimento das configurações e do ambiente para a equipe da CONTRATANTE ou para uma nova empresa.

6.7.2 Entrega de toda a documentação técnica atualizada, como o Caderno de Documentação As Built , e devolução integral de todos os dados de backup da CONTRATANTE que estejam em posse da CONTRATADA, especialmente os armazenados em datacenter externo.

6.7.3 Desinstalação e retirada de todos os equipamentos, produtos e softwares fornecidos em regime de comodato das instalações da CONTRATANTE, garantindo que o ambiente da CONTRATANTE não sofra interrupção ou prejuízo.

Quantidade mínima de serviços para comparação e controle

6.8. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no neste Termo de Referência.

Mecanismos formais de comunicação

6.9. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

- I) Ordem de Serviço;
- II) Ata de Reunião;
- III) Ofício;
- IV) Sistema de abertura de chamados;
- V) E-mails e Cartas;
- VI) WhatsApp.

Manutenção de Sigilo e Normas de Segurança

6.10. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.11. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS: Termo de Compromisso e Manutenção de Sigilo.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto Contratado.

7.6. O Contratado não necessitará manter preposto da empresa no local da execução do objeto.

7.7. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que o Contratado designará outro para o exercício da atividade.

Reunião Inicial

7.8. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições

estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.9. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.10. A pauta desta reunião observará, pelo menos:

7.10.1 Presença do representante legal da contratada, que apresentará o seu preposto;

7.10.2 Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.10.3 esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.10.4 A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.10.5 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Rotinas de Fiscalização

7.11. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.12. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.13. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.14. Identificada qualquer inexistência ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.15. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.16. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

7.18. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

7.18.1 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput)

7.19. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes,

gestores e fiscais, de conformidade.

Fiscalização Administrativa

7.20. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.21. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.22. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

7.22.1 A fiscalização administrativa poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

Gestor do Contrato

7.23. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.23.1 coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.23.2 acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.23.3 acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.23.4 emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.23.5 tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.23.6 elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.23.7 enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

7.23.8 receber e dar encaminhamento imediato:

7.23.8.1. às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;

7.23.8.2. à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR)

IAP - ÍNDICE DE ATENDIMENTO NO PRAZO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na prestação dos serviços constantes na Ordem de Serviço.
Meta a cumprir	IAP igual ou superior a 90%.
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Forma de acompanhamento	É apurado pelos fiscais do contrato avaliando a quantidade atendida dentro do prazo em relação à quantidade total atendida no período de referência.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	$IAP = 100 * (\Sigma Q_{tap} / \Sigma Q_{tr})$ Onde: IAP = Indicador de atendimento aos prazos do serviço; ΣQ_{tap} = Somatório do quantitativo atendido no prazo máximo estabelecido no TR com previsão de encerramento para o período de referência; ΣQ_{tr} = Somatório do quantitativo total registrado com previsão de encerramento para o período de referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da OS.
Faixas de ajuste no pagamento e Sanções	IAP $\geq$ 90%: sem descontos sobre o valor da fatura mensal. IAP $\geq$ 80% e $<$ 90%: 10% de desconto sobre o valor da fatura mensal. IAP $\geq$ 70% e $<$ 80%: 20% de desconto sobre o valor da fatura mensal. IAP $<$ 70%: 30% de desconto sobre o valor da fatura mensal.

8.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que o Contratado:

- não produziu os resultados acordados,
- deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou
- deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

8.3. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

8.4. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

8.4.1 O recebimento provisório dos serviços pelos fiscais técnico e administrativo, que atestarão o cumprimento das exigências de caráter técnico e administrativo, e o subsequente recebimento definitivo por servidor ou comissão designada, que verificará a qualidade e a quantidade do serviço prestado.

8.4.2 A apuração do resultado das avaliações da execução do objeto, realizada pelo fiscal técnico, analisando o desempenho e a qualidade dos serviços com base nos indicadores previstos (como o IAP), o que pode resultar no redimensionamento de valores a serem pagos.

8.4.3 A emissão do Termo Detalhado para efeito de recebimento definitivo, a comunicação à empresa para que emita a Nota Fiscal com o valor exato dimensionado pela fiscalização e a verificação da manutenção da regularidade fiscal da contratada

Recebimento

8.5. Os serviços serão recebidos provisoriamente, no prazo de 10 dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.6. O prazo para recebimento provisório será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.7. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.8. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

8.9. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

8.10. Para efeito de recebimento provisório, será considerado para fins de faturamento o período **mensal de prestação dos serviços**.

8.11. Ao final de cada período/evento de faturamento:

8.12. o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

8.13. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

8.14. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.15. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.16. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.17. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.18. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.19. Os serviços serão recebidos definitivamente no prazo de 30 (trinta) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.20. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

8.20.1 Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;

8.20.2 Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.20.3 Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.20.4 Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.21. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.22. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo Contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.23. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Procedimentos de Teste e Inspeção

8.24. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.24.1 Para a fase de Implantação: A verificação do cumprimento de todas as etapas (Planejamento, Implementação, Testes) , a comprovação de que todos os requisitos técnicos dos itens 2, 3, 4 foram atendidos

8.24.2 Para os Serviços Gerenciados (contínuos): A análise mensal dos relatórios obrigatórios de Firewall e Backup e a verificação do cumprimento dos Acordos de Nível de Serviço (ANS) através da aferição dos registros na ferramenta de chamados.

8.24.3 Para todos os serviços: A comprovação do atendimento aos requisitos será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica e verificação das configurações aplicadas, comparadas aos itens deste Termo.

Liquidação

8.25. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

8.26. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.27. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

- I) o prazo de validade;
- II) a data da emissão;
- III) os dados do contrato e do órgão contratante;
- IV) o período respectivo de execução do contrato;
- V) o valor a pagar; e
- VI) eventual destaque do valor de retenções tributárias cabíveis.

8.28. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

8.29. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

8.30. A Administração deverá realizar consulta ao SICAF para:

- verificar a manutenção das condições de habilitação exigidas;
- identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

8.31. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

8.32. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.33. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

8.34. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

8.35. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.36. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo da Tecnologia da Informação (ICTI) de correção monetária.

Forma de pagamento

8.37. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

8.38. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.39. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

· Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.40. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Antecipação de pagamento

8.41. A presente contratação não permite a antecipação de pagamento parcial ou total.

Reajuste

8.42. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 01/02/2026.

8.43. Após o interregno de um ano, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.44. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.45. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

8.46. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

8.47. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

- 8.48. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
- 8.49. O reajuste será realizado por apostilamento.

Cessão de Crédito

- 8.50. As cessões de crédito dependerão de prévia aprovação do Contratante.
- 8.50.1 A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.
- 8.50.2 Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.
- 8.50.3 O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.
- 8.50.4 A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

8.51. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

9.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

<i>Id</i>	<i>Ocorrência</i>	<i>Glosa / Sanção</i>
<i>1</i>	<i>Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 06 (seis) horas úteis.</i>	<i>Multa de 2% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 10 (dez) dias úteis.</i>
		<i>Após o limite de 11 (onze) dias úteis, aplicar-se-á multa de 10% do valor total do Contrato.</i>
<i>2</i>	<i>Não atender ao indicador de nível de serviço IAP (Índice de Atendimento no</i>	<i>IAP >= 90%: sem descontos sobre o valor da fatura mensal.</i>
		<i>IAP >= 80% e < 90%: 10% de desconto sobre o valor da fatura mensal.</i>

	Prazo)	IAP $\geq$ 70% e $<$ 80%: 20% de desconto sobre o valor da fatura mensal.
		IAP $<$ 70%: 30% de desconto sobre o valor da fatura mensal.
3	<i>Não cumprir qualquer outra obrigação contratual não citada nesta tabela.</i>	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10 (dez) % do valor total do Contrato.

9.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

- não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou
- deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

9.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

9.4.1 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

9.4.2 Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

9.4.3 Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

9.4.3.1. Multa:

9.4.3.2. Moratória, para as infrações descritas no item “d”, de 2% (dois por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias.

9.4.3.3. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

9.4.3.4. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

9.4.3.5. Compensatória, para as infrações descritas nas alíneas “e”, “f”, “g” e “h” de 20% (vinte por cento) a 50% (cinquenta por cento) do valor da contratação.

9.4.3.6. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 10% (dez por cento) a 20% (vinte por cento) do valor da contratação.

9.4.3.7. Compensatória, para a infração descrita acima na alínea “b”, de 10% (dez por cento) a 20% (vinte por cento) do valor da contratação.

9.4.3.8. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 10% (dez por cento) a 20% (vinte por cento) do valor da contratação.

9.4.3.9. Compensatória, para a infração descrita acima na alínea “a”, de 10% (dez por cento) a 20% (vinte por cento) do valor da contratação.

9.4.3.10. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

9.4.3.11. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

9.4.3.12. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.4.3.13. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

9.4.3.14. A multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.4.3.15. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

9.4.3.16. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

9.4.3.17. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

9.4.3.18. Na aplicação das sanções serão considerados:

9.4.3.19. a natureza e a gravidade da infração cometida;

- 9.4.3.20. as peculiaridades do caso concreto;
- 9.4.3.21. as circunstâncias agravantes ou atenuantes;
- 9.4.3.22. os danos que dela provierem para o Contratante; e
- 9.4.3.23. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 9.4.3.24. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.
- 9.4.3.25. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.
- 9.4.3.26. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.
- 9.4.3.27. As penalidades serão obrigatoriamente registradas no SICAF.
- 9.4.3.28. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.
- 9.4.3.29. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio de dispensa eletrônica com fundamento no art. 75, inciso II, da Lei nº 14.133, de 1º de abril de 2021, com base no seguinte fundamento: para contratação que envolva valores inferiores a R\$ 50.000,00 (cinquenta mil reais) (Vide Decreto nº 12.343, de 2024).

Regime de Execução

10.2. O regime de execução do contrato será por empreitada por preço global.

Exigências de habilitação

10.3. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

10.4. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.5. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.6. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

10.7. Sociedade empresária, sociedade limitada unipessoal - SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.8. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.9. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.10. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.11. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

10.12. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021).

10.13. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

10.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.18. Prova de inscrição no cadastro de contribuintes Distrital ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.19. Prova de regularidade com a Fazenda Distrital ou Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.20. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

10.22. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.23. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.24. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

10.25. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, patrimônio líquido mínimo de 10% do valor total estimado da contratação para o período de doze meses.

10.26. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

10.27. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.28. O atendimento dos índices econômicos previstos neste termo de referência deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

10.29. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

Qualificação Técnico

10.30. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

· Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a ao serviços executado(s) com as seguintes características mínimas:

- Não serão aceitos atestados com objeto genérico, ou seja, deverá constar nos respectivos Atestados nomenclatura compatível com os itens licitados. Os atestados deverão ser apresentados em papel timbrado ou com carimbo do CNPJ da pessoa jurídica, contendo a identificação do signatário, ficando reservado à Comissão Permanente de Licitação o direito de solicitar cópias dos contratos e notas fiscais a que se referem tais documentos;

· O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

· Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

10.30.1. Justificativa para a Não Dispensa da Qualificação Técnica: Em que pese a contratação enquadrar-se nas hipóteses de dispensa de licitação em razão do valor ou entrega imediata, mantêm-se as exigências de qualificação técnica descritas neste termo, sendo inviável sua dispensa, dada a alta criticidade e a natureza especializada do objeto (Segurança da Informação e Proteção de Dados). A comprovação da capacidade técnica é indispensável para mitigar riscos de incidentes cibernéticos, vazamento de dados sensíveis (LGPD) e descontinuidade dos serviços públicos do CRM-TO, assegurando que a contratada possua maturidade operacional e certificações técnicas compatíveis com a complexidade do ambiente tecnológico a ser protegido.

10.31. Declaração de que o fornecedor possui ou instalará escritório no município de Palmas - TO, o que deverá ser comprovado no prazo máximo de 60 (sessenta) dias, contado a partir da vigência do contrato.

10.32. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.33. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

Disposições gerais sobre habilitação

10.34. Quando permitida a participação na licitação/contratação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.35. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que

venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.36. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.37. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.38. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

Documentação complementar para cooperativas

10.39. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

- A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

- A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

- A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

- O registro previsto na Lei n. 5.764, de 1971, art. 107;

- A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

- Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

- ata de fundação;
- estatuto social com a ata da assembleia que o aprovou;
- regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;
- editais de convocação das três últimas assembleias gerais extraordinárias;
- três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais;
- ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da contratação; e
- última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação é de R\$ 62.725,72 (sessenta e dois mil setecentos e vinte e cinco reais e setenta e dois centavos), conforme custos unitários apostos em anexo

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos do

12.2. A contratação será atendida pela seguinte dotação:

- I) Elemento de despesa: 6.2.2.1.1.33.90.39.010 - MANUTENÇÃO DE SISTEMAS DE INFORMÁTICA - SOFTWARE.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilas

Integrante Requisitante Athos Alencar de Almeida Assistente de Tecnologia da Informação 78	Integrante Técnico Athos Alencar de Almeida Assistente de Tecnologia da Informação 78	Integrante Administrativo Janderik Silva Marins Assessor Especial I 84
--	---	--

Autoridade Máxima da Área de TIC Wordney Carvalho Camarço Presidente do CRM-TO (em exercício) Portaria SEI-Nº 64/2026
--

Palmas-TO ,02 de julho de 2026.

ANEXO I DO TERMO DE REFERÊNCIA TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

(A ser assinado pelo Representante Legal da Contratada)

Processo Administrativo nº: 25.27.000005403-8

Contratante: CONSELHO REGIONAL DE MEDICINA DO ESTADO DO TOCANTINS (CRM-TO)

Pelo presente Termo, a empresa _____, inscrita no CNPJ sob o nº _____, doravante denominada CONTRATADA, por meio de seu representante legal, assume o compromisso de manter o mais absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas, configurações de rede e credenciais de acesso de que venha a ter conhecimento em razão da execução do Contrato de prestação de Serviços Gerenciados de Segurança da Informação (Firewall e Backup).

A CONTRATADA declara estar ciente de que:

1. É vedada a divulgação, reprodução, utilização ou transmissão de qualquer informação do CRM-TO para fins diversos do cumprimento do objeto contratual, sem expressa autorização.
2. Deverá orientar seus empregados e prepostos quanto à obrigatoriedade de sigilo e cumprimento das normas de Segurança da Informação do CRM-TO, bem como da

Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

3. O não cumprimento deste compromisso sujeitará a CONTRATADA às sanções administrativas, civis e criminais previstas na legislação vigente.

Local e Data: _____, ____ de _____ de 20.

Assinatura do Representante Legal da Contratada

[Nome Completo]

[CPF]

ANEXO II DO TERMO DE REFERÊNCIA TERMO DE CIÊNCIA

(A ser assinado pelos Empregados/Técnicos da Contratada envolvidos na execução)

Processo Administrativo nº: 25.27.000005403-8

Vínculo: _____ Empregado/Preposto _____ da _____ empresa

Eu, _____, portador(a) do CPF nº _____, designado(a) para atuar na execução dos serviços de Segurança da Informação junto ao CRM-TO, DECLARO ter ciência:

1. Da obrigatoriedade de manter sigilo sobre todas as informações, dados e credenciais de acesso aos quais eu tiver acesso durante a execução dos serviços.
2. Das normas de segurança da informação vigentes no CRM-TO e das responsabilidades decorrentes da Lei Geral de Proteção de Dados (LGPD).
3. De que não poderei copiar, transmitir ou divulgar dados do CRM-TO a terceiros não autorizados.

Comprometo-me a utilizar os acessos lógicos e físicos concedidos exclusivamente para as atividades estritamente necessárias ao cumprimento de minhas funções técnicas.

Local e Data: _____, ____ de _____ de 20.

Assinatura do Empregado/Técnico

[Nome Completo]



Documento assinado eletronicamente por **Athos Alencar de Almeida, Assistente de Tecnologia da Informação**, em 02/07/2026, às 14:25, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



Documento assinado eletronicamente por **Janderik Marins, Assessor Especial**, em 02/07/2026, às 14:30, com fundamento no art. 5º da [RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



Documento assinado eletronicamente por **Wordney Carvalho Camarço**,
Presidente do CRM-TO, em 02/07/2026, às 15:03, com fundamento no art. 5º da
[RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022](#).



A autenticidade do documento pode ser conferida no site
[https://sei.cfm.org.br/sei/controlador_externo.php?](https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) informando o código
verificador **4476441** e o código CRC **E12C6455**.



ACSV 71 (704 Sul), Av. LO 15, Lote 18,
1º piso - Bairro Plano Diretor Sul |
CEP 77022-322 | Palmas/TO -
<http://www.crmto.org.br/>



Referência: Processo SEI nº 25.27.000005403-8 | data de inclusão: 02/07/2026