

Tecnologia

Rua Estados Unidos, 889 - Bairro Jardim América - São Paulo-SP - CEP 01427-001

Telefone: (11) 3087-3200 - www.crasp.gov.br

TERMO DE REFERÊNCIA Nº 131/2026/CRA-SP

PROCESSO Nº 476906.000765/2026-33

SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para prestação de serviços de Segurança Cibernética, Governança (GRC) e Auditoria Técnica (Pentest), dividida em 03 (três) grupos, para atender às necessidades do CRA-SP pelo período de 36 (trinta e seis) meses, conforme condições estabelecidas neste instrumento.

1.2.

Grupo	Item	Descrição	CATSER/PDM	Unidade de Medida	Quant.	Valor Unitário	Valor total ESTIMADO (12 MESES)	Valor total ESTIMADO (36 MESES)
1	1	Appliance NGFW (Hardware + Licenças + Garantia) - Mensal	350949	Unidade	1	4.837,29	58.047,48	174.142,44
	2	Licença Endpoint Protection (EPP/EDR/XDR) - Mensal	350949	Pacote com 250	1	4.302,50	51.630,00	154.890,00
	3	Licença ZTNA (Zero Trust) - Mensal	350949	Pacote com 120	1	5.158,11	61.897,32	185.691,96
	4	Serviço de Instalação, Configuração e Migração (incluindo execução de Plano de Rollback, se necessário)	26972	Serviço	1	11.200,00	11.200,00	

	5	Serviço de Suporte Técnico e MDR (Mensal)	16918	Serviço	1	2.243,00	26.916,00	80.748,00
	6	Treinamento e Transferência de Conhecimento	21172	Horas	16	460,00	7.360,00	
2	7	Consultoria em GRC: Elaboração de Diagnóstico de Maturidade, Matriz de Riscos e Plano de Continuidade de Negócios (PCN) com revisão anual. (12 meses) - Ciclo I	13781	Serviço	1	2.533,33	R\$ 30.400,00	-
	8	Ciclo II – Serviço de Suporte Técnico: início após a conclusão do Ciclo I.	16918	Serviço	1	R\$ 4.560,00	R\$ 54.720	R\$ 164.160,00
3	9	Auditoria e Pentest: Execução de testes de invasão e auditoria técnica independente a cada 180 dias.	14168	Ciclo (semestral)	6	9.570,66	19.141,32	57.423,96
VALOR TOTAL							R\$ 321.312,12	R\$ 866.016,36

1.3. O Valor Total estimado para **12 meses** é de **R\$ 321.312,12 (trezentos e vinte e um mil trezentos e doze reais e doze centavos)** e para **36 meses** é de **R\$ 866.016,36 (oitocentos e sessenta e seis mil e dezesseis reais e trinta e seis centavos)**.

1.4. Em caso de eventual divergência entre a descrição do item do catálogo do sistema Compras.gov.br e as disposições deste Termo de Referência, prevalecem as disposições deste Termo de Referência.

1.5. Ressalta-se que a empresa a ser contratada para o Grupo 3 (item 9) não poderá ser a mesma vencedora do Grupo 1, em observância ao princípio da independência técnica.

1.5.1. Tal vedação justifica-se pela necessidade de assegurar a imparcialidade, a confiabilidade dos resultados, especialmente considerando que os serviços previstos no Grupo 3 relacionados à auditoria e testes de invasão, possuem caráter avaliativo e fiscalizador em relação às soluções implementadas no âmbito do Grupo 1.

1.6. Por sua vez, a empresa a ser contratada para os Grupos 1 e 2 poderá ser a mesma, desde que atenda a todos os requisitos estabelecidos no edital.

1.6.1. O(s) serviço(s) objeto desta contratação são caracterizados como **comum(ns)**, conforme justificativa constante do **Estudo Técnico Preliminar, anexo I** desse Termo de Referência.

1.7. **Classificação do objeto quanto ao modelo de execução**

1.7.1. O serviço é enquadrado como continuado, conforme detalhado no Estudo Técnico Preliminar, anexo I deste Termo de Referência.

1.8. **Prazo de vigência**

1.8.1. O contrato terá vigência inicial de 36 (**trinta e seis**) meses, contados a partir da data de sua assinatura, podendo ser prorrogado por até 10 (dez) anos, desde que comprovada a vantajosidade do preço, nos termos do art. 107 da Lei nº 14.133/2021.

2. **DESCRIÇÃO DA NECESSIDADE E FUNDAMENTAÇÃO DA CONTRATAÇÃO**

2.1. O CRA-SP é uma autarquia federal, organizada na forma de Conselho de Fiscalização Profissional (CFP) que orienta, disciplina e fiscaliza o exercício profissional da área de Administração, matéria de sua competência.

2.2. Como prestador de um serviço público, o CRA-SP desenvolve relevantes atividades dentro de sua jurisdição, ou seja, no estado de São Paulo, por meio da fiscalização do exercício profissional. Como os demais Conselhos de Fiscalização Profissional, sua receita é uma verba pública de caráter tributário, usada exclusivamente para a manutenção de suas atividades essenciais.

2.3. O CRA-SP é uma entidade dotada de personalidade jurídica de direito público, com autonomia técnica, administrativa e financeira e não recebe nenhuma subvenção do governo federal, tendo todo seu recurso alicerçado nos tributos pagos pelos administradores.

2.4. Conforme acima exposto, para que nossas atividades finalísticas sejam bem cumpridas, faz-se necessária a complementação com atividades meio, ou seja, aquelas que possibilitam e criam condições favoráveis para o funcionamento da Entidade.

2.5. O CRA-SP possui atualmente uma infraestrutura de segurança baseada em tecnologias legadas (VPNs tradicionais e firewalls de borda simples), que se mostram insuficientes diante da crescente sofisticação de ataques cibernéticos (Ransomwares, Phishing avançado) e da nova realidade de trabalho híbrido. A necessidade fundamenta-se em:

2.5.1. Vulnerabilidade Tecnológica: A ausência de inspeção profunda de tráfego criptografado e de ferramentas de detecção e resposta (MDR) expõe os ativos de informação do Conselho a riscos críticos;

2.5.2. Mitigar o risco de interrupção dos serviços essenciais prestados pelo CRA-SP à sociedade devido a incidentes de segurança;

2.5.3. Gestão de Identidade e Acesso: Com o aumento do trabalho remoto, o modelo de VPN atual é baseado em confiança implícita na rede. A necessidade é migrar para o conceito de Zero Trust Network Access (ZTNA), onde o acesso é concedido por usuário e dispositivo, e não por rede.

2.5.4. A contratação de serviços de GRC justifica-se pela necessidade de atender ao princípio da continuidade do serviço público e às diretrizes de governança do Tribunal de Contas da União (TCU), suprimindo a ausência de um Plano de Continuidade de Negócios (PCN) e de indicadores de desempenho (KPIs) de segurança, elementos essenciais para a prestação de contas (Accountability) exigida pelas Instruções Normativas do Governo Federal e pela LGPD.

2.6. **Fundamentação**

2.6.1. A contratação será realizada com fundamento no art. 28, inciso I, da Lei nº 14.133/2021.

2.7. A contratação supracitada está prevista no plano de contratações anual (PCA) de 2026 do CRA-SP, conforme item 10 do Estudo Técnico Preliminar, anexo I deste Termo de Referência.

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

3.1. Arquitetura e Integração: A solução foi desenhada sob o conceito de Defesa em Profundidade, estruturada em três pilares complementares que garantem a resiliência tecnológica do CRA-SP:

3.1.1. Pilar de Proteção e Operação (Grupo 1): Implementação de uma arquitetura SASE (Secure

Access Service Edge) e Zero Trust. O hardware (Firewalls) é fornecido como serviço (HaaS), garantindo que o Conselho tenha sempre tecnologia de ponta. A operação é reforçada pelo serviço de MDR, que provê monitoramento e resposta a incidentes 24x7, suprimindo a carência de equipa interna para vigilância noturna e de fins de semana.

3.1.2. Pilar de Estratégia e Normatização (Grupo 2): A consultoria em GRC atuará na camada intelectual, definindo as políticas, analisando riscos e criando o Plano de Continuidade de Negócios (PCN). Esta camada garante que as ferramentas do Grupo 1 estejam alinhadas aos objetivos estratégicos e de adequação (LGPD) do Conselho.

3.1.3. Pilar de Validação e Auditoria (Grupo 3): Através de Pentests semestrais, uma empresa independente testará a eficácia das defesas implementadas no Grupo 1 e a aderência aos processos do Grupo 2, fechando o ciclo de melhoria contínua (PDCA).

3.2. Modelo de Entrega e Sustentabilidade: A solução será entregue predominantemente no modelo de Serviço (OpEx). Esta escolha garante a Sustentabilidade Tecnológica (evitando hardware obsoleto parado em inventário) e a Sustentabilidade Ambiental, uma vez que a logística reversa e o descarte de resíduos eletrônicos ficam a cargo da contratada do Grupo 1, conforme o Guia Nacional de Contratações Sustentáveis.

3.3. Transferência de Conhecimento: Para garantir que o CRA-SP não sofra de "aprisionamento tecnológico" (vendedor lock-in), a solução prevê a transferência de conhecimento técnico através de formações gravadas e entrega de documentação técnica exaustiva.

3.4. Pertinência Técnica: Ao descrever a solução como um "todo", justificamos porque é que a contratação não pode ser apenas um "antivírus" ou apenas um "firewall" isolado.

3.5. **Local da prestação dos serviços:**

3.5.1. Os serviços serão prestados no Conselho Regional de Administração de São Paulo (CRA-SP), localizado na Rua Estados Unidos, 889, Jardim América, São Paulo - SP, CEP 01427-001.

3.6. **Materiais a serem disponibilizados**

3.6.1. Não se aplica.

4. REQUISITOS DA CONTRATAÇÃO

4.1. **São responsabilidades da contratada para o grupo 1:**

4.1.1. Planejamento e Migração (Turn-Key):

4.1.1.1. Após a convocação, firmar o contrato ou instrumento substitutivo em até 5 dias úteis;

4.1.1.2. Mapeamento e migração de todas as regras de firewall, NATs, rotas e VPNs atualmente em produção na solução legada para a nova solução.

4.1.1.3. Revisão e saneamento das regras ("limpeza"), eliminando regras obsoletas, duplicadas ou permissivas demais (ex: 'Any-Any'), seguindo as boas práticas de segurança.

4.1.1.4. Desinstalação assistida da solução de antivírus atual e instalação dos novos agentes de Endpoint/XDR em 100% (cem por cento) do parque computacional (Estações e Servidores), salvo exceções justificadas de sistemas operacionais legados nos quais a referida implementação seja técnica e comprovadamente inviável, garantindo-se, em todo caso, a não interrupção das atividades dos usuários.

4.1.1.5. Deverá apresentar, no Plano de Trabalho inicial, uma metodologia detalhada de migração 'Turn-Key', contendo obrigatoriamente um Plano de Rollback, em até 2 dias úteis após o início do contrato.

4.1.2. **Implantação ZTNA:**

4.1.2.1. Configuração das políticas de acesso Zero Trust para todos os usuários remotos, incluindo integração com o diretório de usuários (AD/LDAP) e configuração de Múltiplo Fator de Autenticação (MFA).

4.1.3. **Treinamento:**

4.1.3.1. Realização de treinamento técnico para a equipe de TI do CRA-SP sobre a operação e gestão da nova solução.

4.1.4. **Operação assistida:**

4.1.4.1. Acompanhamento presencial ou remoto dedicado por período mínimo de 5 (cinco) dias úteis após a virada de chave (Go-Live) para resolução imediata de eventuais instabilidades.

4.1.5. **Especificação Técnica: Firewall NGFW (grupo 1):**

4.1.5.1. O equipamento ofertado deve ser um appliance físico (hardware) dedicado de segurança, de arquitetura moderna, atendendo aos seguintes requisitos mínimos de performance e hardware, visando suportar a carga atual e expansão futura dos links de comunicação (300 Mbps com previsão de upgrade).

4.1.6. **Performance**

4.1.6.1. Throughput de Threat Prevention (considerando IPS, Controle de Aplicação, Anti-Malware e SSL Inspection ativados): Mínimo de 2,5 Gbps.

4.1.6.2. Throughput de Firewall (UDP): Mínimo de 5 Gbps.

4.1.6.3. Conexões Simultâneas: Mínimo de 1.500.000.

4.1.6.4. Throughput de VPN (IPSec): Mínimo de 1.5 Gbps.

4.1.6.5. Novas Conexões por Segundo: Mínimo de 25.000.

4.1.7. **Hardware**

4.1.7.1. Interfaces: Mínimo de 8 portas 1GbE (RJ45) e 2 portas 10GbE (SFP+).

4.1.7.2. Armazenamento interno (SSD/Flash) para logs locais e quarentena.

4.1.7.3. Fonte de Alimentação Redundante (interna ou externa).

4.1.7.4. Formato: Rackmount 1U (Alternativamente, será admitido equipamento em formato desktop, desde que acompanhado de kit original do fabricante para montagem em rack)

4.1.8. **Funcionalidades de Segurança:**

4.1.8.1. Inspeção Profunda de Pacotes (DPI): Tecnologia de inspeção de pacotes sem remontagem (Reassembly-Free ou tecnologia de passagem única) para garantir baixa latência e alta performance.

4.1.8.2. Inspeção SSL/TLS: Capacidade de descriptografar e inspecionar tráfego criptografado (TLS 1.3) sem degradação superior a 50% do throughput nominal.

4.1.8.3. Sandboxing em Nuvem (ATP): Recurso de análise de ameaças desconhecidas (Zero-Day) em ambiente isolado na nuvem (Sandbox), com capacidade de inspeção de memória em tempo real para detecção de malwares evasivos.

4.1.8.4. IPS (Intrusion Prevention System): Proteção contra exploits, vulnerabilidades e ataques de rede.

4.1.8.5. Gateway Anti-Malware: Detecção e bloqueio de vírus, worms e outros malwares no tráfego de rede.

4.1.8.6. Controle de Aplicação: Identificação e controle de mais de 3.000 aplicações.

4.1.8.7. Filtro de Conteúdo Web: Bloqueio de acesso a categorias de sites maliciosos ou indesejados.

4.1.8.8. VPN (Virtual Private Network): Suporte a VPN IPSec e SSL VPN para acesso remoto seguro.

4.1.8.9. SD-WAN Nativo: Funcionalidades de SD-WAN, permitindo balanceamento de links baseado em performance (jitter, latência, perda de pacotes) e identificação de aplicações.

4.1.9. **Especificação Técnica: Endpoint/XDR (grupo 1)**

4.1.9.1. Proteção Multicamada: Deve utilizar combinação de aprendizado de máquina (Machine Learning), análise comportamental (Heurística) e reputação em nuvem. Não serão aceitas soluções baseadas exclusivamente em assinaturas.

4.1.9.2. Anti-Ransomware: Módulo específico de proteção contra ransomware com capacidade de detecção de criptografia não autorizada e rollback (reversão) de arquivos criptografados via Shadow Copy ou tecnologia proprietária.

4.1.9.3. Devem ser compatíveis com Windows 10, Windows 11 e versões posteriores; macOS (versões

estáveis atuais), distribuições Linux e macOS.

4.1.9.4. Devem ser compatíveis com Windows Server 2012, 2016, 2019, 2022 e versões posteriores, estendendo-se o requisito de compatibilidade aos demais sistemas operacionais legados vigentes na infraestrutura do órgão, salvo exceções justificadas de sistemas operacionais legados nos quais a referida implementação seja técnica e comprovadamente inviável.

4.1.9.5. Controle de Dispositivos: Capacidade de controlar o uso de dispositivos removíveis (USB, CD/DVD).

4.1.9.6. Firewall de Host: Firewall pessoal integrado para controle de tráfego de rede no endpoint.

4.1.9.7. Gerenciamento Centralizado em Nuvem (Cloud Management):

4.1.9.8. A solução deve prover console de gerenciamento centralizado 100% baseado em nuvem (SaaS), acessível via navegador web, sem a necessidade de instalação de servidores locais.

4.1.9.9. Comunicação Híbrida: Os agentes devem se comunicar com a console via Internet, independentemente de estarem na rede local ou em roaming, sem necessidade de VPN.

4.1.9.10. Gestão de Políticas: A console deve permitir a criação, edição e aplicação granular de políticas de segurança (ex: controle de dispositivos, exclusões de varredura, bloqueio de aplicações) para grupos de dispositivos ou usuários específicos.

4.1.9.11. Dashboards e Relatórios: Deve fornecer painéis gráficos (dashboards) em tempo real com visão geral do estado de segurança do parque, além de permitir a geração e exportação de relatórios gerenciais e técnicos (ex: Top Ameaças, Status de Atualização, Dispositivos Infectados).

4.1.9.12. Alertas e Notificações: Capacidade de envio automático de alertas (por e-mail ou na própria console) em caso de detecção de infecções críticas, surtos de malware ou falhas de conformidade.

Ações Remotas: A console deve permitir ao administrador executar tarefas de resposta remotamente, incluindo: iniciar varreduras (scans) sob demanda, forçar atualização de assinaturas, isolar o host da rede, reiniciar o dispositivo e executar ações de desinfecção/quarentena de arquivos.

4.1.10. **Especificação Técnica: ZTNA (grupo 1)**

4.1.10.1. Acesso Mínimo Privilegiado: O acesso deve ser concedido a aplicações específicas (segmentação por aplicação) e não à rede corporativa inteira, baseando-se na identidade do usuário e contexto.

4.1.10.2. Verificação de Postura (Device Posture Check): A solução deve verificar a saúde do dispositivo (ex: Antivírus ativo, SO atualizado, Disco criptografado) antes e durante a conexão. Dispositivos fora de conformidade devem ter o acesso negado ou restrito automaticamente.

4.1.10.3. Autenticação Contínua: Revalidação constante da identidade e postura durante a sessão, não apenas no login inicial.

4.1.10.4. A solução deve ser gerida através de console centralizada em nuvem (SaaS), permitindo a administração de políticas de acesso de qualquer local.

4.1.10.5. Gestão de Políticas Granulares: Deve permitir a criação de políticas de acesso baseadas em múltiplos critérios: Identidade do Usuário (Grupo AD), Tipo de Dispositivo, Localização Geográfica e Horário de Acesso.

4.1.10.6. Dashboards e Visibilidade: A console deve apresentar dashboards com visão em tempo real dos usuários conectados, aplicações acessadas, tentativas de acesso bloqueadas e falhas de postura de segurança.

4.1.10.7. Relatórios de Auditoria: Capacidade de gerar relatórios detalhados de auditoria de acesso, registrando “Quem acessou O Que e Quando”, para fins de conformidade e investigação forense.

4.1.10.8. Autenticação: Suporte nativo a Múltiplo Fator de Autenticação (MFA) e integração transparente com diretórios de usuários (Active Directory/LDAP/Azure AD).

4.1.10.9. Aplicação obrigatória de 2FA/MFA para Área de Trabalho Remota (RDP), acessos remotos, VPN e demais recursos corporativos protegidos pela solução.

4.1.10.10. Experiência do Usuário: Deve suportar acesso via agente (Client) para aplicações legadas (Client-Server) e acesso sem agente (Clientless/Browser-based) para aplicações Web, garantindo facilidade de uso.

4.1.10.11. A solução de ZTNA deve possuir integração (nativa ou via conectores documentados) com o Firewall para compartilhamento automático de postura e contexto de segurança.

4.1.11. **Especificação do serviço de Suporte Técnico, operação assistida e MDR (grupo 1):**

4.1.11.1. O serviço deve contemplar a Operação Assistida e Administração Continuada de todos os componentes da Solução Integrada (Firewall, Endpoint e ZTNA), abrangendo as seguintes responsabilidades:

4.1.11.2. Gestão de Firewall (NGFW): Criação, alteração e otimização de regras, NAT, rotas, VPNs (Site-to-Site e Client-to-Site) e políticas de segurança.

4.1.11.3. Gestão de Endpoint e ZTNA: Criação e manutenção de políticas de proteção, gestão de exceções, configuração de grupos de usuários, verificação de postura e regras de acesso remoto.

4.1.11.4. Atualização de Software: Planejamento e execução de atualizações de Firmware, Agentes e Patches de todos os componentes (Appliance e Softwares), garantindo versões estáveis e seguras.

4.1.11.5. Abrangência Geral: A responsabilidade da Contratada inclui, ainda, tudo mais que for pertinente à administração, manutenção, operação, configuração e sustentação de todos os produtos e serviços que compõem o Grupo 1 (Firewall, Endpoint, ZTNA e correlatos), garantindo seu pleno funcionamento e aderência às necessidades de negócio do CRA-SP.

4.1.11.6. Considerando a função de Gateway/Roteador da solução, o suporte deverá estender-se à camada de rede (L2/L3) necessária para a integração.

4.1.11.7. Escopo de Atuação na LAN: Configuração e troubleshooting de VLANs (802.1Q), interfaces virtuais, Roteamento Inter-VLAN, rotas estáticas e protocolos de roteamento dinâmico.

4.1.11.8. Diagnóstico: Análise de problemas de conectividade, perda de pacotes ou latência envolvendo o tráfego da solução.

4.1.11.9. Vedação de Escopo: Fica vedado encerrar chamados alegando "problema na rede interna" sem comprovação técnica (logs/pcap) de que a falha não reside nos equipamentos ou softwares da solução contratada.

4.1.11.10. Monitoramento 24x7x365, análise de incidentes e resposta a ameaças nos ambientes de Borda, Endpoint, Acesso Remoto e Nuvem (Google Workspace).

4.1.11.11. Os serviços deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

4.1.11.12. O Serviço de Suporte Técnico, operação assistida e MDR terá início após a entrega dos serviços referentes aos itens (1, 2, 3, 4 e 6) e a devida validação/homologação pela área de Tecnologia do CRA-SP.

4.1.12. **Especificação Técnica: Consultoria GRC (grupo 2):**

4.1.12.1. Diagnóstico de Maturidade (Gap Analysis): Relatório técnico contendo o levantamento da situação atual (As-Is) dos processos de segurança e privacidade do CRA-SP em relação às normas ISO/IEC 27001, 27002 e LGPD, com identificação de lacunas e recomendações de correção. Confeccionando artefatos em caso de inexistência ou necessidade.

4.1.12.2. Inventário de Dados e Ativos (Data Mapping/ROPA): Mapeamento do ciclo de vida dos dados pessoais e sensíveis e inventário de ativos de TI. Entrega do ROPA (Registro de Operações de Tratamento) conforme Art. 37 da LGPD e Art. 103 da Lei 14.133/21 (Matriz de Riscos).

4.1.12.3. Metodologia de Classificação da Informação: Elaboração da Matriz de Classificação da Informação (ex: Público, Interno, Confidencial) e definição de regras de etiquetamento para subsidiar a configuração de ferramentas de DLP (Data Loss Prevention).

4.1.12.4. Plano Diretor de Segurança da Informação (PDSI): Elaboração de planejamento estratégico específico para Segurança da Informação, contendo diretrizes, metas, indicadores (KPIs) e roadmap de investimentos para o horizonte de 24 a 60 meses.

4.1.12.5. Política de Segurança e Normas (PSI): Revisão e/ou elaboração da Política de Segurança da Informação (PSI) e normas acessórias (Uso de Ativos, Senhas, Home Office, BYOD), com minuta pronta para aprovação da Alta Administração.

4.1.12.6. Relatório de Impacto (RIPD/DPIA): Elaboração do Relatório de Impacto à Proteção de Dados Pessoais para os processos críticos identificados, contendo análise de necessidade, proporcionalidade e riscos aos titulares (Art. 38 LGPD).

4.1.12.7. Plano de Continuidade (PCN/DR): Elaboração do Plano de Continuidade de Negócios e Recuperação de Desastres, definindo estratégias de backup, RTO/RPO e procedimentos de acionamento em crises.

4.1.12.8. Workshop de Conscientização: Realização de ciclo de palestras/treinamento para colaboradores sobre as novas políticas e boas práticas de segurança (Cultura de Segurança).

4.1.12.9. Requisito de Aceite (grupo 2): Todos os produtos deverão ser entregues em formato editável, acompanhados de reunião de transferência de conhecimento gravada. O pagamento será vinculado à homologação/entrega formal de cada produto pelo Fiscal de Contrato e o Gestor do Contrato.

4.2. **Da Execução e Continuidade dos Serviços de Governança (grupo 2):**

4.2.1. Os serviços de Consultoria em Governança, Riscos e Conformidade (GRC) serão prestados de forma continuada pelo período de 36 (trinta e seis) meses, estruturados em dois ciclos operacionais:

4.2.2. Ciclo I - de Implementação (Meses 1 a 12): Destinado à execução do diagnóstico inicial e entrega formal dos produtos listados no item **4.1.12 (Especificação Técnica: Consultoria GRC (grupo 2))**.

4.2.3. Ciclo II - de Sustentação e Melhoria (Meses 13 a 36): Destinado à manutenção da conformidade alcançada, compreendendo as seguintes obrigações mensais:

4.2.3.1. Gestão de Mudanças Normativas: Atualização imediata de políticas e regramentos internos frente a novas resoluções da ANPD ou alterações legislativas;

4.2.3.2. Suporte Consultivo On-Demand: Disponibilidade de consultoria técnica para responder a questionamentos da TI ou da Diretoria sobre privacidade de dados e segurança da informação;

4.2.3.3. Tratamento de Gap Analysis: Revisão anual do diagnóstico de maturidade e ajuste do plano de ação com base nas vulnerabilidades identificadas pelos Pentests semestrais (Grupo 3);

4.2.3.4. Apoio em Incidentes de Privacidade: Suporte especializado na elaboração de comunicações à ANPD e aos titulares em caso de incidentes de dados ocorridos durante a vigência.

4.2.3.5. A CONTRATADA deverá manter canal de comunicação ativo (e-mail e reuniões mensais de status) para garantir que a governança de dados acompanhe o crescimento institucional e as mudanças na infraestrutura tecnológica do CRA-SP.

4.2.4. O faturamento deste grupo deverá observar o, **Cronograma Físico-Financeiro de Execução dos Serviços e Entrega dos Produtos (Grupo 2), anexo VIII** desse Termo de Referência.

4.3. **Especificação Técnica: Auditoria e testes de invasão (grupo 3) - item 9:**

4.3.1. Serviço de Teste de Invasão (Pentest): Realização de testes de invasão em aplicações web, infraestrutura e rede interna.

4.3.2. Tipos de Teste: Deverá contemplar testes Black Box (sem conhecimento prévio), Grey Box (com conhecimento parcial) e White Box (com conhecimento total do ambiente), tentativas de exploração manual, engenharia social e demais testes de vulnerabilidades de segurança que forem necessários.

4.3.3. Áreas de Abrangência: Aplicações web (se houver), infraestrutura de rede (servidores, dispositivos de rede) e rede interna (segmentos de LAN).

4.3.4. Relatório Técnico Detalhado: Contendo a metodologia utilizada, descrição das vulnerabilidades encontradas, nível de risco (CVSS ou similar), evidências (screenshots, logs) e recomendações técnicas de correção.

4.3.5. Relatório Executivo: Sumário gerencial com os principais achados, impacto no negócio e plano de ação recomendado para a Alta Administração.

4.3.6. Re-teste (Retest): Realização de reteste para validação da correção das vulnerabilidades críticas identificadas no relatório inicial.

4.3.7. Evidências de: Exploração Manual, Engenharia Social e Demais testes além dos mecânicos e automatizados através de ferramentas.

4.3.8. Periodicidade: Os testes deverão ser realizados a cada 180 dias (6 meses) durante a vigência do contrato.

4.3.9. É vedada a entrega de relatórios provenientes exclusivamente de scanners automatizados. A Contratada deverá comprovar a execução de testes manuais, com tentativas de exploração (exploitation) de

falhas lógicas e de negócio, evidenciando o sucesso ou insucesso da intrusão."

4.3.10. O faturamento deste grupo deverá observar o **Cronograma Físico-Financeiro de Execução dos Serviços e Entrega dos Produtos (grupo 3) - item 9, anexo IX** desse Termo de Referência.

4.4. **Requisitos de Segurança da Informação e LGPD**

4.4.1. A Contratada deverá cumprir rigorosamente as diretrizes de segurança da informação do CRA-SP e as disposições da Lei Geral de Proteção de Dados Pessoais (LGPD). Deverá assinar Termo de Confidencialidade, anexo III e de Tratamento de Dados anexo IV desse termo de Referência, comprometendo-se a processar os dados (logs) exclusivamente para a finalidade contratual, garantindo a confidencialidade, integridade e disponibilidade das informações,

4.5. **Obrigações da Contratante:**

4.5.1. Disponibilizar acesso lógico e físico, quando necessário, para a execução dos serviços.

4.5.2. Designar um fiscal do contrato para acompanhar e fiscalizar a execução do objeto.

4.5.3. Prestar as informações e esclarecimentos necessários à Contratada.

4.5.4. Efetuar os pagamentos devidos conforme as condições contratuais.

4.6. **Obrigações da Contratada:**

4.6.1. Executar o objeto com a máxima diligência, qualidade e observância das normas técnicas e legais.

4.6.2. Manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação.

4.6.3. Responsabilizar-se integralmente pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

4.6.4. Garantir a confidencialidade das informações do CRA-SP.

4.6.5. Disponibilizar equipe técnica qualificada para a execução dos serviços.

4.6.6. Prestar esclarecimentos que forem solicitados pelo CRA-SP;

4.6.7. Zelar pelo sigilo inerente à execução do objeto e pela confidencialidade quanto aos dados e informações do CRA-SP, empregando todos os meios necessários para tanto;

4.6.8. Manter durante toda a execução do objeto, todas as condições de habilitação e qualificação exigidas para sua contratação em compatibilidade com as obrigações assumidas;

4.7. **Garantia da contratação**

4.7.1. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, uma vez que o objeto licitatório não envolve o fornecimento de mão de obra com dedicação exclusiva, tampouco apresentam riscos que seriam indenizados com aplicação da garantia da execução, considerando o valor da Solução Integrada de Segurança Cibernética e Serviços Especializados de Governança e Auditoria serem contratados.

4.8. **Vistoria**

4.8.1. 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 9 horas às 17 horas, conforme **modelo anexo V** desse Termo de Referência.

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

b) 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.

4.8.2. 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, conforme

modelo anexo VI desse Termo de Referência.

4.8.3. 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.

4.9. **De sustentabilidade**

4.9.1. Os equipamentos fornecidos no modelo HaaS (Grupo 1) devem possuir eficiência energética e baixo consumo elétrico nominal, visando a redução do impacto ambiental no Data Center do CRA-SP. A comprovação de eficiência poderá ser atendida mediante a apresentação do datasheet oficial do fabricante ou declaração técnica equivalente, dispensada a obrigatoriedade de selos comerciais específicos.

4.9.2. Conforme a Lei nº 12.305/2010, a CONTRATADA é integralmente responsável pela destinação final dos equipamentos obsoletos ou substituídos durante a vigência contratual.

4.9.3. Ao fim do contrato ou na substituição de componentes (ex: baterias, placas, appliances), a CONTRATADA deverá realizar a recolha e o descarte em conformidade com as normas ambientais, apresentando o comprovante de descarte adequado à fiscalização do CRA-SP.

4.10. **Subcontratação**

4.10.1. Não será admitida a subcontratação do objeto contratual.

5. **MODELO DE EXECUÇÃO DOS SERVIÇOS**

5.1. **Condições de execução**

5.1.1. **A execução do objeto seguirá a seguinte dinâmica:**

5.1.1.1. **Início da execução do objeto:** em até 5 (cinco) dias úteis a partir da assinatura do contrato.

5.1.1.2. O Envio do contrato e/ou ordem de serviço assinado será realizado por meio eletrônico, conforme o e-mail informado na proposta comercial.

5.1.1.3. **Prazos de Entrega (Grupo 1):** A entrega dos equipamentos e licenças deve ocorrer em até 30 (trinta) dias corridos após a assinatura do contrato.

5.1.1.4. **Instalação (Kick-off):** O início da instalação deve ocorrer em até 5 (cinco) dias úteis após o recebimento provisório dos equipamentos.

5.1.1.5. **Conclusão e Go-Live:** A migração e implantação total devem ser concluídas em até 30 (trinta) dias corridos após o início da instalação.

5.1.1.6. **Gestão do contrato:** Ficará a cargo de empregado público devidamente designado pela Administração.

5.2. **Informações relevantes para o dimensionamento da proposta**

5.2.1. Para a elaboração da proposta comercial, as licitantes deverão considerar as seguintes particularidades do ambiente do CRA-SP, conforme as informações apresentadas a seguir e modelo **Anexo VII** desse Termo de Referência.

5.2.2. **Conectividade:** O órgão possui links de comunicação de 300 Mbps, com previsão de upgrade, que devem ser suportados pelo hardware ofertado.

5.2.3. **Parque Computacional:** A licitante deve prever o licenciamento e suporte para 250 endpoints (estações e servidores) e 120 usuários de acesso remoto ZTNA.

5.2.4. **Sistemas Legados:** Os sistemas operacionais Windows Server 2008, 2008 R2, 2012 e 2012 R2 ainda compõem a infraestrutura crítica do Conselho. Caso as limitações tecnológicas desses sistemas legados

representem um impedimento técnico intransponível para a instalação dos agentes de segurança padrão, o requisito de proteção exigido para estes servidores específicos poderá ser atendido por meio da instalação de agentes legados de proteção (Antivírus/EPP) ou, de forma complementar e alternativa, por mecanismos equivalentes de proteção e isolamento lógico na camada de rede (como inspeção profunda, segmentação por Firewall, DMZ ou *Virtual Patching*). Tais mecanismos de mitigação e isolamento deverão ser obrigatoriamente providos e gerenciados através da própria solução integrada de Firewall (NGFW) exigida no Grupo 1 deste Termo de Referência, garantindo que não haja risco de exposição cruzada. Para todos os demais ativos da rede, mantém-se a exigência rigorosa de proteção multicamadas e comportamental (EDR/XDR).

5.2.5. Ecosistema Cloud: A solução deve integrar-se via API com a suíte Google Workspace utilizada pelo Contratante.

5.2.6. Localidade: Os serviços presenciais (quando necessários) serão prestados no Conselho Regional de Administração de São Paulo, na rua Estados Unidos, 889, Jardim América, São Paulo - SP.

5.3. Especificação da garantia do serviço

5.3.1. Grupo 1:

5.4. O prazo de garantia contratual dos serviços do Grupo 1, complementar à garantia legal, será de, no mínimo, 36 (trinta e seis) meses, (ou tempo total de vigência do contrato), contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

5.4.1. A garantia deve cobrir todo o período de vigência para assegurar a continuidade operacional da Solução Integrada de Segurança. Para o hardware (Item 1) do Grupo 1, a garantia deve incluir substituição avançada (RMA). A substituição avançada (RMA) deverá ocorrer no modelo NBD (Next Business Day - Próximo Dia Útil) após a constatação da falha de hardware.

5.5. Procedimentos de transição e finalização do contrato

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

5.5.2. Transferência de Conhecimento: Realização de reuniões técnicas e entrega de documentação exaustiva das configurações (firewall, políticas de ZTNA e Endpoint), com sessões gravadas e manuais atualizados.

5.5.3. Entrega de Artefatos (Grupo 2): Todos os produtos de consultoria (PSI, PCN, Inventário) devem ser entregues em formato editável.

5.5.4. Logística Reversa (Sustentabilidade): No encerramento do contrato, a contratada do Grupo 1 é responsável pela recolha e descarte ambientalmente adequado de todos os equipamentos fornecidos no modelo HaaS, conforme a Lei nº 12.305/2010.

5.5.5. Plano de Desmobilização: Apresentação de um cronograma de 30 dias para a migração assistida dos serviços para um novo prestador, se aplicável, sem interrupção da proteção do CRA-SP.

6. MODELO DE GESTÃO DO CONTRATO

6.1. 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.

6.2. 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.

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

6.4. O CRA-SP poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.6. **Preposto**

6.6.1. Não se aplica.

6.7. **Rotinas de Fiscalização**

6.7.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos.

6.7.2. **Fiscalização Técnica**

6.7.2.1. 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.

6.7.2.2. O fiscal técnico do contrato anotará 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.

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

6.7.2.4. 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.

6.7.2.5. 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.

6.7.2.6. 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.

6.7.2.7. 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.

6.7.2.8. As disposições previstas neste Termo de Referência não excluem o disposto no Anexo VIII da Instrução Normativa SEGES/MP nº 05, de 2017, aplicável no que for pertinente à contratação, por força da Instrução Normativa Seges/ME nº 98, de 26 de dezembro de 2022.

6.7.3. **Fiscalização Administrativa**

6.7.3.1. O fiscal administrativo do contrato 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.

6.7.3.2. 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.

6.7.4. **Gestor do Contrato**

6.7.4.1. Cabe ao gestor do contrato:

- a) 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.
- b) 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.
- c) 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.
- d) 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.
- e) 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.
- f) 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.
- g) Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.
- h) Receber e dar encaminhamento imediato:
 - I - às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;
 - II - 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.

7. RECEBIMENTOS PROVISÓRIO DO OBJETO

- 7.1. Os serviços serão recebidos provisoriamente, no prazo de **5 (cinco) dias**, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. ([Art. 140, I, a, da Lei nº 14.133, de 2021](#) e [Arts. 22, X e 23, X do Decreto nº 11.246, de 2022](#)).[A1]
- 7.2. O prazo da disposição acima 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.
- 7.3. 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. ([Art. 22, X, Decreto nº 11.246, de 2022](#)).
- 7.4. 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. ([Art. 23, X, Decreto nº 11.246, de 2022](#)).
- 7.5. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.
- 7.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá 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, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

7.6.1. 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;

7.6.2. 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.

7.6.3. 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. ([Art. 119 c/c art. 140 da Lei nº 14133, de 2021](#))

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

7.6.5. 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.

7.6.6. 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. RECEBIMENTO DEFINITIVO DO OBJETO

8.1. Os serviços serão recebidos definitivamente no prazo de **5 (cinco) 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:

8.1.1. 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 ([art. 21, VIII, Decreto nº 11.246, de 2022](#)).

8.1.2. 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 à CONTRATADA, por escrito, as respectivas correções;

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

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

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

8.2. 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 no que pertence à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

8.4. 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.

9. PAGAMENTO

9.1. Liquidação

9.1.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de **10 (dez) dias úteis** para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

9.1.2. 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.

9.1.3. 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:

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão contratante;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar; e
- f) eventual destaque do valor de retenções tributárias cabíveis.

9.1.4. 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 à contratante;

9.1.5. 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.

9.1.6. A Administração deverá realizar consulta ao SICAF para:

- a) verificar a manutenção das condições de habilitação exigidas no edital ou instrumento equivalente;
- b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

9.1.7. 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.

9.1.8. 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.

9.1.9. 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.

9.1.10. 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.

9.2. **Prazo de pagamento**

9.2.1. O pagamento será efetuado no prazo máximo de até **30 (trinta) dias**, após a emissão da nota fiscal, de acordo com as descrições contidas na Nota de Empenho, contrato ou outro instrumento hábil.

9.2.2. 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 IPCA de correção monetária.

9.3. **Forma de pagamento**

9.3.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

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

9.3.4. 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.

9.3.5. 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.

10. REAJUSTE

10.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 09/04/2026.

10.2. 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.

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

10.4. 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).

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

10.6. 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.

10.7. 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.

10.8. O reajuste será realizado por termo aditivo.

11. FORMA E CRITÉRIOS DE SELEÇÃO E REGIME DE EXECUÇÃO

11.1. Forma de seleção e critério de julgamento da proposta

11.2. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

11.3. **Regime de execução**

11.4. Empreitada por preço unitário:

11.5. O regime de execução do contrato ou de outro instrumento hábil equivalente será EMPREITADA POR PREÇO UNITÁRIO.

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

12.1. O Valor Total estimado para 12 meses é de R\$ 321.312,12 (trezentos e vinte e um mil trezentos e doze reais e doze centavos) e para 36 meses é de R\$ 866.016,36 (oitocentos e sessenta e seis mil e dezesseis reais e trinta e seis centavos).

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos próprios.

13.2. A contratação será atendida pela seguinte dotação, conforme:

13.2.1. **6.2.2.1.1.01.04.04.037 - Serviços de Internet e Data Center**

13.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação do Orçamento.

14. ANEXOS:

I - Estudo Técnico Preliminar da Contratação - ETP-TIC 5 (3968897);

II - Mapa de Risco (3968910)

III - Termo de Compromisso de Confidencialidade e Sigilo 3 (3969245);

IV - Termo de especificação de troca de inf. conf. (3969261);

V - Atestado de Vistoria - (3969266);

- VI - Atestado de Vistoria de Não Realização - (3969275);
- VII - Modelo de Proposta de Preço - Licitação - (3969285);
- VIII - Cronograma Físico de execução dos serviços/entrega - Grupo 2 - (3969293);
- IX - Cronograma Físico de execução dos serviços/entrega - Grupo 3 - (3969303);
- X - Minuta de Contrato - (3969312);

São Paulo, 8 de maio de 2026.

Eduardo S. Borghi Kondo
Assessor de Tecnologia

Ivan Cesar Machado Narciso
Coordenador de Infraestrutura



Documento assinado eletronicamente por **Ivan Cesar Machado Narciso, Coordenador(a) de Infraestrutura Computacional**, em 08/06/2026, às 11:13, conforme horário oficial de Brasília.



Documento assinado eletronicamente por **Eduardo Sadayoshi Borghi Kondo, Gerente de Tecnologia**, em 08/06/2026, às 11:24, conforme horário oficial de Brasília.



A autenticidade deste documento pode ser conferida no site sei.cfa.org.br/conferir, informando o código verificador **4118880** e o código CRC **EA6E5CB2**.