

# Termo de Referência 24/2024

## Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
24/2024	173039-MF-SUSEP-SUPERINT.DE SEGUROS PRIVADOS/RJ	LUIZ EDUARDO ADEMI TEIXEIRA	02/10/2024 12:15 (v 3.0)
Status	ASSINADO		

## Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		15414.652048/2023-16

## 1. TERMO DE REFERÊNCIA SERVIÇOS DE TIC

### TERMO DE REFERÊNCIA SERVIÇOS DE TIC – LEI 14.133/2021

(Processo Administrativo nº 15414.626758/2023-82)

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

### 1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa especializada para prestação de serviços de hospedagem de aplicações e soluções de TIC em data center da Contratada (hosting), para atender às necessidades da Susep - Superintendência de Seguros Privados, conforme condições e exigências estabelecidas neste instrumento.

Item	CATSER	Unidade	Quantidade	Valor Total (36 meses)
1 - Serviços de Hospedagem de Sistemas.	27065	Un	1	R\$ 17.224.350,60

1.2. O objeto será adjudicado pelo menor preço global, respeitando os valores máximos por item e subitem, conforme especificações constantes neste Termo de Referência e na planilha de custos em anexo a este documento.

1.3. A planilha de custos é parte integrante da proposta de preços e contém o detalhamento, os quantitativos e custos dos serviços a serem contratados.

1.4. Os serviços objeto desta contratação são caracterizados como comuns, uma vez que há padrões de mercado e, que permitem a fixação de padrões de qualidade e de desempenho para o referido serviço.

1.5. O prazo de vigência da contratação é de 36 (trinta e seis) meses, contados da data de início da vigência do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.6. O Contrato poderá ser rescindido unilateralmente pela CONTRATANTE após decorridos no mínimo 24 (vinte e quatro) meses de vigência contratual e comunicação prévia à CONTRATADA com antecedência mínima de 90 (noventa) dias. A CONTRATADA deverá, a partir de 24 (vinte e quatro) meses de início de vigência do Contrato, informar o interesse na sua prorrogação em até 10 (dez) dias úteis após a solicitação da CONTRATANTE.

1.7. O serviço é enquadrado como natureza contínua, pois visa assegurar a sustentação da infraestrutura tecnológica e de sistemas computacionais, cenário no qual sua eventual paralisação ou descontinuidade podem implicar prejuízos às atividades do órgão, sendo a vigência plurianual mais vantajosa considerando o Estudo Técnico Preliminar.

1.8. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

## 2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

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

### 2.2. Descrição do Ambiente

2.2.1. O ambiente deve estar localizado em infraestrutura física tradicional de data center de propriedade da CONTRATADA, sem o compartilhamento de recursos entre clientes, na qual seja possível executar estes recursos em uma rede virtual definida pela CONTRATANTE.

2.2.2. A CONTRATADA deverá possuir, no mínimo, 2 (dois) data centers de sua propriedade com os seguintes requisitos:

2.2.2.1. no mínimo 1 (um) data center primário em território brasileiro com certificação Tier III (Tier Standards) ou Tier 3 (EIA /TIA 942) para hospedagem do ambiente da CONTRATANTE em alta disponibilidade;

2.2.2.2. no mínimo 1 (um) data center em território brasileiro, diferente do anterior, para recuperação de desastres (disaster recovery) com ambiente stand-alone para receber a replicação do data center primário e hospedagem da infraestrutura de backup no qual haverá o armazenamento de cópia de segurança (backup) do servidores. As capacidades de Internet, firewall e WAF precisam ser iguais nos dois sites.

2.2.3. Os data centers da CONTRATADA deverão estar em conformidade com os padrões de segurança, por meio de auditoria anual SOC-2, conduzida por um auditor independente, com a apresentação do relatório de tipo II.

2.2.4. Os equipamentos e appliances do ambiente deverão ser de uso exclusivo e dedicado da CONTRATANTE, incluindo servidores, storages, switches, firewalls e WAF (web application firewall). Será admitido somente o compartilhamento de racks, instalações elétricas e dos links de acesso do data center à internet. A CONTRATADA permitirá o acesso ao ambiente físico dos equipamentos sempre que solicitado pela CONTRATANTE após agendamento prévio.

2.2.5. O serviço de hospedagem contemplará, sem ônus adicional para a CONTRATANTE, fornecimento, configuração, sustentação e manutenção de recursos de hardware e software, armazenamento, atualização de versões, acesso à internet, segurança, gerenciamento, processamento dos dados, configuração de endereçamento IP, subredes, serviços de proxy, serviço de resolução de nomes (DNS), Firewall, VPN e WAF.

2.2.6. O DNS interno da CONTRATADA deve ser configurado em pelo menos dois servidores distintos por questões de contingência. Deve haver um servidor mestre com autoridade sobre uma determinada zona cujos dados são derivados dos arquivos locais e outro equipamento distinto utilizado como secundário (slave).

2.2.7. A CONTRATANTE possui 2 domínios ativos no RegistroBR. No tocante ao serviço externo de resolução de nomes (DNS Externo), a CONTRATADA deverá prover servidores Name Server (NS), para resolução pública dos domínios da CONTRATANTE, bem como dos subdomínios ativos e os que futuramente vierem a ser solicitados pela CONTRATANTE. Ainda, a CONTRATANTE poderá fazer encaminhamento de requisição DNS para os servidores de DNS público da CONTRATADA.

2.2.8. A CONTRATADA deverá prestar suporte de infraestrutura ao servidor de relay SMTP (Simple Mail Transfer Protocol) da CONTRATANTE, permitindo que aplicações efetuem o envio de e-mails para endereços internos e externos, de acordo com as regras a serem definidas pela CONTRATANTE para cada aplicação, cabendo à CONTRATANTE a gestão da mensageria encaminhada.

2.2.8.1. Atualmente a CONTRATANTE possui servidor de relay SMTP via IIS de servidor Windows Server 2019 e uso do Conector de fluxo de e-mail do Exchange Online (Office 365) através do serviço AD Connect. Compete à CONTRATADA gerenciar a requisição de remoção de possíveis adições do domínio da SUSEP em listas denominadas BlackLists, bem como implementar configurações recomendadas para evitar novas inclusões.

2.2.9. A CONTRATADA deverá prestar suporte à administração de servidores onde os Websites da CONTRATANTE (Microsoft IIS, Apache, etc.) estiverem instalados no ambiente da CONTRATADA, desenvolvidos nas tecnologias ASP, .NET, PHP, Python e Java.

2.2.10. A CONTRATADA deverá manter atualizados tecnologicamente todos os ativos de hardware e software estabelecidos neste documento, destinados à execução dos serviços disponíveis no Centro de Dados, configurando as últimas versões, atualizações ou correções recomendadas (hardware/software), de modo a assegurar a plena integridade do ambiente. Os procedimentos de atualização seguirão a GMUD (Gestão de Mudanças) da CONTRATANTE.

2.2.11. A CONTRATADA deverá se utilizar de processos de monitoramento, gerência de falhas e de mudanças, além de possibilitar a verificação dos NÍVEIS MÍNIMOS DE SERVIÇO (NMS) objeto desta contratação.

2.2.12. A CONTRATADA deverá submeter à aprovação da CONTRATANTE as paradas programadas de equipamentos ou serviços com antecedência mínima de 2 (dois) dias úteis.

2.2.13. Em caso de paradas emergenciais, a qualquer tempo, a CONTRATADA deverá realizar os serviços de manutenção corretiva, quando possível, em finais de semana ou em dias úteis após as 19h00, mitigando a indisponibilidade dos sistemas e acesso à internet. Tais paradas deverão ser previamente aprovadas pela CONTRATANTE.

2.2.14. O serviço de hospedagem de sistemas e gerenciamento do centro de dados, contemplará ainda as seguintes rotinas:

2.2.14.1. Operação de servidores, equipamentos de interconexão de rede e periféricos em geral.

2.2.14.2. Administração e manutenção das bases e bancos de dados da CONTRATANTE.

2.2.14.3. Monitoração de servidores, disponibilidade de serviços (sistema operacional, banco de dados, sites web, firewall, WAF, links de acesso e outros ativos do ambiente contratado) e alerta de eventos relacionados ao ambiente definido pela CONTRATANTE.

2.2.14.4. Administração do diretório de usuários (Active Directory).

2.2.15. A CONTRATADA disponibilizará, mensalmente ou sempre que solicitada, relatório gerencial dos incidentes e solicitações abertas, para que a CONTRATANTE possa atestar o provimento dos serviços. Além disso, para fins de controle e auditoria, a CONTRATADA deve disponibilizar as informações supracitadas para a equipe técnica da CONTRATANTE, a qualquer tempo, através de sistema informatizado, incluindo o fornecimento de dados quanto aos níveis de serviço alcançados pelos serviços fornecidos pela CONTRATADA.

2.2.16. A CONTRATADA deverá participar, quando solicitada, de reuniões eventuais ou regulares com os gerentes e participantes dos projetos de desenvolvimento, manutenção, administração de dados, sustentação e segurança da informação, a fim de apoiar a elaboração de soluções para atividades em andamento.

2.2.17. Todas as ferramentas de gerenciamento e monitoração a serem fornecidas pela CONTRATADA deverão permitir acesso de leitura para a equipe técnica da CONTRATANTE para a verificação e validação dos serviços prestados.

2.2.18. Os equipamentos e appliances fornecidos para atendimento dos serviços (servidores de rede, armazenamento, switches, roteadores, etc.) deverão ser sempre novos, em primeiro uso, estar cobertos por garantia contratual pelos fabricantes e não poderão estar em fim de ciclo vida de suporte (end of live).

2.2.19. A configuração e manutenção da infraestrutura dos servidores, serão de responsabilidade da CONTRATADA e deverão seguir diretrizes definidas pela CONTRATANTE.

2.2.20. A CONTRATADA deverá garantir que estrutura do ambiente esteja disponível por pelo menos 99,982% do tempo anual, devendo, quando solicitada, encaminhar os projetos e documentos que demonstrem a citada disponibilidade. O ambiente será provido com redundância, replicação de ambientes, tolerância a falhas e recuperação de desastres sem custo adicional para a CONTRATANTE.

2.2.21. A CONTRATADA deverá manter atualizada a topologia com todos os recursos físicos e virtuais do ambiente fornecido. Esta topologia, quando solicitada, deverá ser entregue no prazo máximo de 2 (dois) dias úteis, contados da solicitação pela CONTRATANTE.

2.2.22. Os ambientes (produção, homologação e desenvolvimento) devem ser segregados, impedindo-se a comunicação entre as máquinas localizadas em ambientes distintos. Esta segregação deve ser feita através de firewall ou protocolo 802.1q de modo que seja possível, a critério da CONTRATANTE, controlar através de listas de controle de acesso (ACLs) o tráfego entre as diversas máquinas hospedadas, de acordo com as sub-redes de origem e destino e os protocolos utilizados (ICMP, TCP, UDP e respectivas portas).

2.2.23. A CONTRATADA deve prover mecanismos de alertas baseados no gerenciamento de métricas. Caso uma métrica (uso de disco, processamento ou memória) exceda certo valor, alerta deve ser gerado com envio de e-mail para destinatários definidos pela CONTRATANTE.

2.2.24. A CONTRATADA deve prover, sem ônus adicional para a CONTRATANTE, mecanismos de monitoração de métricas e de segurança de todos os recursos providos no ambiente de data center, tais como: quantidade de acessos, utilização de CPU, leitura/escrita em disco e disponibilidade do serviço.

2.2.25. As máquinas virtuais deverão ser providas com Sistemas Operacionais descritos neste Termo de Referência.

2.2.26. Quando solicitada, a CONTRATADA deverá realizar a clonagem, importação e/ou exportação de máquinas virtuais sem ônus adicional para a CONTRATANTE, devendo esta informar o local e destino dos respectivos clones gerados.

2.2.27. Máquinas virtuais devem possibilitar a utilização de sistemas operacionais Windows Server 2019 Data Center (ou superior) e Red Hat Enterprise Linux. As licenças para as máquinas virtuais com Sistema Operacional Windows Server Data Center, Red Hat Enterprise Linux e SQL Server Enterprise deverão compor o preço da máquina virtual. A CONTRATADA deverá manter o suporte ativo junto aos fabricantes das licenças fornecidas.

2.2.28. A CONTRATADA deverá prover mecanismos de monitoração de métricas dos serviços, tais como: quantidade de acessos, erros, porcentagem de disponibilidade do serviço e utilização de rede.

2.2.29. As interfaces de rede das máquinas virtuais devem permitir a criação de regras de firewall que liberem ou bloqueiem o tráfego de entrada e/ou saída a determinadas portas, a determinados IPs ou faixas de IPs.

2.2.30. A CONTRATADA deverá disponibilizar, sem ônus adicional para a CONTRATANTE, sistema WEB em tempo real para monitoramento, análise e armazenamento de logs, gerência de falhas e de mudanças, além de possibilitar a verificação dos NÍVEIS MÍNIMOS DE SERVIÇOS (NMS).

2.2.31. Cabe à CONTRATADA a aplicação de patches, correções e atualizações dos sistemas operacionais, bem como suas dependências, para prover de forma funcional e segura, o perfeito funcionamento das máquinas virtuais nas versões mais atualizadas. Os procedimentos serão realizados de acordo com o cronograma aprovado pela CONTRATANTE.

2.2.32. As políticas aplicáveis aos ativos de segurança do ambiente serão implementadas pela CONTRATADA, que deverá possuir pessoal qualificado à operação do ambiente descrito, de acordo com as regras definidas pela CONTRATANTE.

2.2.33. A CONTRATADA deverá ainda:

2.2.33.1. utilizar-se de melhores práticas e tecnologias reconhecidas pelo mercado no sentido de gerir e operacionalizar a segurança da informação e comunicação, bem como de prevenir incidentes;

2.2.33.2. tratar Incidentes de segurança (vírus, spam, phishing e outros) em conjunto com o pessoal técnico da CONTRATANTE;

2.2.33.3. consolidar relatórios mensais de ataques e incidentes para apresentação à CONTRATANTE;

2.2.33.4. proteger todos os componentes da solução CONTRATADA (hardware e software) contra vulnerabilidades conhecidas e que venham a ser divulgadas pelos fabricantes;

2.2.33.5. nos casos de resposta a ataques e vulnerabilidades que ensejarem intervenção na infraestrutura, a CONTRATANTE deverá ser imediatamente comunicada.

2.2.34. As solicitações de alterações, exclusões e inclusões de novas regras, como, por exemplo, filtros de pacotes, bloqueios de endereço IP e fixação de endereço IP e NAT, deverão ser avaliadas e efetivamente operacionalizadas pela CONTRATADA, em um prazo máximo de 1 (um) dia útil.

2.2.35. Qualquer alteração a ser efetuada no ambiente da CONTRATANTE pela CONTRATADA deverá ser previamente autorizada.

### 2.3. Características Mínimas dos Servidores Virtuais

2.3.1. O fornecimento das instâncias computacionais relativas a cada servidor virtual seguirá o seguinte critério (exemplo):

*Máquina provisionada com Linux RHEL, com 8vcpus e 32GB de RAM utilizará 4 blocos de 2vcpus e 8GB de RAM constante do subitem 1.2 da planilha de custos.*

2.3.2. O provisionamento ou exclusão de Servidores Virtuais deverá ser realizado a pedido da CONTRATANTE devendo sempre ser respeitados os prazos previstos no NÍVEL MÍNIMO DE SERVIÇOS constante deste Termo.

2.3.3. Exclusivamente para o caso do subitem 1.3 da planilha de custos (Linux Free), a CONTRATANTE, poderá solicitar a instalação de máquinas virtuais usando imagens do tipo VA - virtual appliance com sistema operacional licenciado para a CONTRATANTE ou terceiros prestadores de serviço à mesma, incluindo imagens KVM (kernel based virtual machine), executadas sobre o virtualizador requisitado neste documento.

2.3.4. O servidor virtual deve possuir endereços IP exclusivos e fixos. Estes endereços não poderão ser atribuídos nem compartilhados com outros recursos computacionais virtuais ou físicos presentes na mesma rede.

2.3.5. A critério da CONTRATANTE, um servidor virtual localizado na DMZ (zona desmilitarizada) poderá possuir dois tipos de IP: público e privado. O endereço IP público será utilizado para endereçamento virtual na Internet, já o endereço IP privado será utilizado para endereçamento na rede interna.

2.3.6. A CONTRATADA deverá fornecer, sem ônus adicional para a CONTRATANTE, uma quantidade mínima de 50 (cinquenta) IP's públicos para as máquinas virtuais da CONTRATANTE, não sendo considerados nesta contagem os IP's públicos referentes aos equipamentos de rede, links IP, firewalls e monitoramento de ativos, a cargo exclusivo da CONTRATADA.

2.3.7. A CONTRATADA deverá fornecer, instalar e manter software antimalware e antivírus de amplo reconhecimento e utilização pelo mercado em todas as máquinas virtuais do ambiente sem ônus adicional para a CONTRATANTE.

2.3.8. A CONTRATADA deverá fornecer suporte à instalação e administração de containers (Docker, Kubernetes, Podman, etc) nas máquinas virtuais fornecidas neste documento.

2.3.9. O ratio, relação entre CPUs físicas (pCPU) e virtuais (vCPU) deverá ser no máximo 4:1 (quatro para um), sendo vedado à CONTRATADA utilizar o ratio superior a este valor.

2.3.10. Os processadores físicos utilizados para o provimento de máquinas virtuais devem possuir processador de clock mínimo de 2.0 GHz (Frequência Básica) e a memória RAM deverá ser do tipo DDR5.

2.3.11. As portas de comunicação da rede LAN (Local Area Network) deverão ser redundantes e possuir velocidades mínimas de 10 (dez) Gbps.

## 2.4. Firewall

2.4.1. O serviço de firewall tem como objetivo atuar como primeira linha de defesa contra ataques ao ambiente hospedado na CONTRATADA. O firewall deve ser capaz de proteger contra uma ampla gama de ataques maliciosos e ser configurado para atender às necessidades específicas da CONTRATANTE. Também estão contempladas neste serviço conexões VPN client-to-site e site-to-site.

2.4.2. A CONTRATADA poderá utilizar appliances virtuais ou físicos, desde que atenda a todos os requisitos deste documento.

### 2.4.3. Funções Básicas

2.4.3.1. Serviços e funcionalidades de firewall que atuam na segurança e performance do ambiente de rede;

2.4.3.2. Alta Disponibilidade;

2.4.3.3. Proxy Web e Filtro de Conteúdo Web (URL Filtering);

2.4.3.4. Controle de Aplicações;

2.4.3.5. VPN SSL, VPN IPSec (Client-to-site e Site-to-site);

2.4.3.6. Detecção e prevenção de intrusos – IDS/IPS;

2.4.3.7. Qualidade de serviço – QOS;

2.4.3.8. Anti-Malware.

#### 2.4.4. **Características Gerais**

2.4.4.1. A solução deve contemplar Serviços e Funcionalidades de Firewall de proteção de rede com funcionalidades de proteção de próxima geração NFWG com detecção e correção avançada de ameaças;

2.4.4.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos destas especificações técnicas;

2.4.4.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, devem ser gerenciadas e configuradas através de um portal e que através dele, as configurações são descarregadas em um único appliance ou em múltiplos appliances desde que obedeçam a todos os requisitos destas especificações técnicas;

2.4.4.4. Os recursos que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores de rede e sistema operacional de uso genérico;

2.4.4.5. A Solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

2.4.4.6. Realizar upgrade via SCP, SFTP ou https via interface WEB;

2.4.4.7. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

2.4.4.8. Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

2.4.4.9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

2.4.4.10. Enviar logs para sistemas de monitoração externos, tais como ferramentas SIEM, simultaneamente;

2.4.4.11. A solução fornecida deve ser compatível com ferramentas de SIEM;

2.4.4.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing);

2.4.4.13. Deve realizar roteamentos unicast e encaminhamento multicast simultaneamente ou bridge em uma única instância (contexto) de firewall;

2.4.4.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

2.4.4.15. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

2.4.4.16. Suportar OSPF graceful restart;

2.4.4.17. Suportar autenticação OSPFv3 AH para protocolo OSPFv3;

2.4.4.18. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6;

2.4.4.19. A Solução deve suportar Dual stack ipv4/ipv6 e NAT64;

2.4.4.20. Deve suportar NAT64 ou NAT46;

2.4.4.21. Deve implementar Network PrefixTranslation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

2.4.4.22. Possibilitar a implementação de políticas de segurança orientadas a credenciais de usuários através de autenticação em diretório padrão Microsoft Active Directory da CONTRATANTE, independentemente do endereço IP de origem e sem necessidade de instalação de agentes nos clientes.

2.4.4.23. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras;

2.4.4.24. A Solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

2.4.4.25. A Solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

2.4.4.26. A Solução deve comportar armazenamento de logs de auditoria das atividades administrativas por pelo menos 30 dias.

2.4.4.27. Deve possuir mecanismo de ativação de validação da regra com período customizado.

#### 2.4.5. **Alta Disponibilidade**

2.4.5.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Failover;

2.4.5.2. Não serão permitidas soluções de cluster (HA) que façam com que o equipamento/appliance reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.

2.4.5.3. O sincronismo dos appliances de firewall devem ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

2.4.5.4. No modo Ativo/Ativo deve permitir a persistência da sessão autenticada dos usuários a manutenção do estado das conexões;

2.4.5.5. No caso de falha do H.A. Ativo Primário, o H.A. Ativo secundário deve assumir de uma forma transparente sem impacto ao usuário ou perda de serviço;

2.4.5.6. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over;

2.4.5.7. O Sincronismo dos servidores deve ser por interface exclusiva permitindo utilizar mais de uma interface de Heartbeat;

#### 2.4.6. **Funcionalidade de Proxy e Filtro de Conteúdo WEB**

2.4.6.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança;

2.4.6.2. Possuir pelo menos 75 categorias para classificação de sites web;

2.4.6.3. Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;

2.4.6.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

2.4.6.4.1. Webmail;

2.4.6.4.2. Instituições de Saúde;

2.4.6.4.3. Notícias;

2.4.6.4.4. Pornografia;

2.4.6.4.5. Restaurante;

2.4.6.4.6. Mídias Sociais;

2.4.6.4.7. Esporte;

2.4.6.4.8. Educação;

2.4.6.4.9. Games;

2.4.6.4.10. Compras.

2.4.6.5. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

2.4.6.6. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

2.4.6.7. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

- 2.4.6.8. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- 2.4.6.9. Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
- 2.4.6.10. Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- 2.4.6.11. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- 2.4.6.12. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- 2.4.6.13. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- 2.4.6.14. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de Active Directory;
- 2.4.6.15. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 2.4.6.16. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- 2.4.6.17. Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- 2.4.6.18. Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam;
- 2.4.6.19. Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- 2.4.6.20. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;
- 2.4.6.21. Deverá permitir configurar Proxy Explícito;

2.4.7. **Funcionalidade de alta disponibilidade (HA) e balanceamento de carga**

- 2.4.7.1. Suporte à configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo: Em modo Transparente: Em Layer 2 e Em Layer 3.
- 2.4.7.2. O HA deve sincronizar:
- 2.4.7.3. Todas as sessões;
- 2.4.7.4. Todas as Associações de Segurança das VPNs;
- 2.4.7.5. Todas as assinaturas de Antivírus, Anti-spyware, Aplicações Web 2.0 e IPS.
- 2.4.7.6. O HA (modo de Alta-Disponibilidade) deve possibilitar tracking de IP.
- 2.4.7.7. Monitoração de falha de link.
- 2.4.7.8. Para melhor desempenho ou em caso de crescimento da rede, a solução deve suportar mais de dois membros no cluster de NG Firewall.
- 2.4.7.9. A solução deve suportar port-aggregation de interfaces de firewall com os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces.
- 2.4.7.10. Suportar agregação de links 802.3ad.

2.4.8. **Funcionalidade VPN (Virtual Private Network)**

- 2.4.8.1. Suportar VPN Site-to-Site e Client-To-Site;
- 2.4.8.2. Suportar IPSec VPN;
- 2.4.8.3. A solução deve suportar Autoridade Certificadora Externa (de terceiros);
- 2.4.8.4. Suportar SSL VPN;



- 2.4.8.5. Suportar IPsec;
- 2.4.8.6. Suportar conexões VPN com AWS - Amazon Web Services;
- 2.4.8.7. A VPN IPSEC deve suportar: 3DES, Autenticação MD5, SHA-1, SHA-256 E SHA-512, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;
- 2.4.8.8. A VPN SSL deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 2.4.8.9. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 2.4.8.10. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;
- 2.4.8.11. Permitir a verificação de conformidade do cliente;
- 2.4.8.12. Atribuição de endereço IP nos
- 2.4.8.13. clientes remotos de VPN;
- 2.4.8.14. Atribuição de DNS nos clientes remotos de VPN;
- 2.4.8.15. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
- 2.4.8.16. Suportar autenticação via RADIUS e LDAP e base de usuários local;;
- 2.4.8.17. Suportar autenticação multifator via Azure AD, tokens OTP, SAML e certificados digitais;
- 2.4.8.18. Suportar leitura e verificação de CRL (certificate revocation list);
- 2.4.8.19. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 10 ou superior, MacOS X, Android e Linux;
- 2.4.8.20. A solução deve estar habilitada e licenciada para utilização de VPN SSL para funcionar com no mínimo 500 (quinhentos) usuários concorrentes ou 2.000 (dois mil) não concorrentes;
- 2.4.8.21. A solução deve comportar armazenamento de logs de auditoria no mínimo dos eventos de login/logoff por pelo menos 30 dias.
- 2.4.9. **Funcionalidade da Detecção de Intrusão**
  - 2.4.9.1. A Detecção de Intrusão deverá ser baseada em appliance fornecida como serviço;
  - 2.4.9.2. Possuir no mínimo 15.000 (quinze mil) assinaturas ou regras de IPS/IDS;
  - 2.4.9.3. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
  - 2.4.9.4. Possuir tecnologia de detecção baseada em assinatura;
  - 2.4.9.5. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;
  - 2.4.9.6. Suportar implementação de cluster do IPS em linha se o equipamento possuir interface do tipo by-pass;
  - 2.4.9.7. O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
  - 2.4.9.8. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv4 e IPv6;
  - 2.4.9.9. Possuir capacidade de remontagem de pacotes para identificação de ataques;
  - 2.4.9.10. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
  - 2.4.9.11. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

- 2.4.9.12. Mecanismos de detecção/proteção de ataques;
- 2.4.9.13. Reconhecimento de padrões;
- 2.4.9.14. Análise de protocolos;
- 2.4.9.15. Detecção de anomalias;
- 2.4.9.16. Detecção de ataques de RPC (Remote procedure call);
- 2.4.9.17. Proteção contra-ataques de Windows ou NetBios;
- 2.4.9.18. Proteção contra-ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- 2.4.9.19. Proteção contra-ataques DNS (Domain Name System);
- 2.4.9.20. Proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- 2.4.9.21. Proteção contra-ataques de ICMP (Internet Control Message Protocol); Alarmes na console de administração;
- 2.4.9.22. Alertas via correio eletrônico;
- 2.4.9.23. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- 2.4.9.24. Capacidade de resposta/logs ativa a ataques;
- 2.4.9.25. Terminação de sessões via TCP resets;
- 2.4.9.26. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 2.4.9.27. A Solução deve comportar armazenamento de logs das anomalias detectadas por pelo menos 30 dias.
- 2.4.9.28. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- 2.4.9.29. Possuir filtros de ataques por anomalias;
- 2.4.9.30. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- 2.4.9.31. Permitir filtros de anomalias de protocolos;
- 2.4.9.32. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- 2.4.9.33. Suportar verificação de ataque nas camadas de aplicação;
- 2.4.10. **Funcionalidade de QoS**
  - 2.4.10.1. Adotar solução de Qualidade de Serviço baseada em appliance;
  - 2.4.10.2. 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, gerência de congestionamento e QoS;
  - 2.4.10.3. Permitir modificação de valores DSCP;
  - 2.4.10.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
  - 2.4.10.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
  - 2.4.10.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
  - 2.4.10.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

2.4.10.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

2.4.10.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

2.4.11. **Funcionalidade de Detecção e Correção Avançada de Ameaças – Threat Protection**

2.4.11.1. Possuir funções de Antivírus, Anti-spyware;

2.4.11.2. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;

2.4.11.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);

2.4.11.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

2.4.11.5. Permitir o bloqueio de download de arquivos por tamanho;

2.4.11.6. Deverá suportar o bloqueio de endereços IP's baseado em sua reputação;

2.4.12. **Funcionalidade do Controle de Aplicações**

2.4.12.1. As funcionalidades abaixo devem ser baseadas em appliance:

2.4.12.2. Deverá reconhecer no mínimo 4000 aplicações;

2.4.12.3. Deverá possuir pelo menos 18 categorias para classificação de aplicações;

2.4.12.4. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

2.4.12.5. P2P;

2.4.12.6. Web;

2.4.12.7. Transferência de arquivos;

2.4.12.8. Chat;

2.4.12.9. Social;

2.4.12.10. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

2.4.12.11. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

2.4.12.12. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

2.4.12.13. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

2.4.12.14. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

2.4.12.15. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

2.4.12.16. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

2.4.12.17. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

2.4.13. A CONTRATADA deverá licenciar e disponibilizar recursos adequados, conforme detalhamento:

2.4.13.1. A vazão de tráfego (throughput) inspecionado pela solução de firewall deve ser, no mínimo, 100% superior ao link de internet fornecido pela CONTRATADA conforme especificado no tópico 2.14 deste documento.

2.5. **WAF - Web Application Firewall**

- 2.5.1. O serviço de blindagem de vulnerabilidades em aplicações web (WAF/WAAP) tem como objetivo proteger aplicações web e APIs contra ataques, atuando como um filtro entre o usuário e a aplicação web, monitorando o tráfego e bloqueando solicitações maliciosas.
- 2.5.2. Serão aceitas soluções em hardware ou software, desde que atendam os requisitos deste documento.
- 2.5.3. A Plataforma de proteção deve ser não intrusiva, ou seja, não ter a necessidade de instalação de agentes ou outros softwares nos servidores da CONTRATANTE. Mas a possibilidade de verificação intrusiva deve ser prevista em casos que isso traga informações mais detalhadas e ficando à critério da CONTRATANTE decidir se utiliza de modo intrusivo ou não intrusivo;
- 2.5.4. A Plataforma de proteção deve garantir alto desempenho de acesso (baixo tempo de carga das páginas) independentemente de quantidade de usuários e de dados acessados simultaneamente, apresentando delay máximo de 500 milissegundos;
- 2.5.5. A Plataforma de proteção deve disponibilizar ferramenta para monitoramento real das informações dos usuários, a partir dos servidores de borda da própria rede de distribuição.
- 2.5.6. A Plataforma de proteção deve prover a infraestrutura necessária para a adequada prestação dos serviços indicados anteriormente, de forma escalável, automaticamente e em tempo real, independentemente da quantidade de acessos simultâneos;
- 2.5.7. A plataforma deverá disponibilizar meios de notificação de alertas das seguintes categorias:
- 2.5.7.1. Quando sites são adicionados ou removidos da plataforma;
- 2.5.7.2. Notificação em tempo real de ataques ocorrendo nas aplicações protegidas pela plataforma.
- 2.5.8. A plataforma deve permitir a criação de usuários com perfis de acesso distintos.
- 2.5.9. A plataforma deve possuir logs administrativos de todas as alterações realizadas pelos administradores.
- 2.5.9.1. A Solução deve comportar armazenamento de logs de auditoria das atividades administrativas e das anomalias detectadas por pelo menos 30 dias.
- 2.5.10. A plataforma deve possuir Dashboard acessível através de Browser o qual permita:
- 2.5.10.1. Analisar o histórico de tráfego (hits, requisições e throughput por segundo);
- 2.5.10.2. Analisar alertas e configurações das políticas de segurança;
- 2.5.10.3. Analisar em tempo real as requisições recebidas pela plataforma, distinguindo a porcentagem de tráfego real e malicioso bem como a porcentagem de tráfego sendo provido pelo cache;
- 2.5.10.4. Analisar o log de requisições legítimas e maliciosas que acessaram a plataforma.
- 2.5.11. As configurações realizadas pelos administradores devem ser propagadas instantaneamente para todos os data centers da plataforma.
- 2.5.12. A defesa da solução deve disponibilizar que todos os servidores da Plataforma de proteção sejam capazes de monitorar, alertar e impedir atividades maliciosas direcionadas aos servidores da CONTRATANTE através de um Web Application Firewall;
- 2.5.13. A solução deverá ter recursos avançados de geração de relatórios claros, de fácil entendimento e atender a conformidades regulatória, permitindo gerar relatórios personalizados ou pré-definidos.
- 2.5.14. A defesa da solução deve ser capaz de correlacionar ataques com precisão, por meio da competência de aprender todos os aspectos do aplicativos WEB, incluindo diretórios, URLs, parâmetros e entrada de usuários aceitáveis, bem como a validação de ataques correlacionando e analisando as violações de forma individuais ou combinadas para detectar ataques com maior precisão e bloquear apenas tráfego malicioso tendo como finalidade a minimização de falsos positivos.
- 2.5.15. A defesa da solução deve ser capaz de filtrar e proteger os ataques direcionados a vulnerabilidade da aplicação, respeitando os padrões da indústria sendo capaz de identificar, alertar e impedir que o acesso malicioso seja realizado, garantindo no mínimo o bloqueio dos grupos de regras listadas, independente do volume:
- 2.5.15.1. Violação por anomalias de protocolo, incluindo inexistência do header na requisição;

2.5.15.2. Bloqueio de tentativas de SQL Injection;

2.5.15.3. Bloqueio de tentativas de Cross Site Script;

2.5.15.4. Bloqueio de Command Injections;

2.5.15.5. Bloqueio de acesso de Trojan;

2.5.15.6. Bloqueio de Backdoors.

2.5.16. A defesa da solução deve ser capaz de proteger os ataques direcionados à camada de aplicação, alertando e/ou bloqueando por acessos excessivos de um único requisitante ou IP, antes que o acesso chegue a infraestrutura de origem possibilitando aplicar as seguintes regras:

2.5.16.1. Identificação do acesso para alerta e/ou bloqueio através do IP do usuário;

2.5.16.2. Identificação do acesso para alerta e/ou bloqueio através da sessão do usuário;

2.5.16.3. Identificação do acesso para alerta e/ou bloqueio através do cruzamento de IP do usuário e um determinado User Agent específico.

2.5.16.4. Identificação do acesso para alerta e/ou bloqueio de requisições com cabeçalhos excessivos.

2.5.17. A defesa da solução deve ser capaz de possibilitar ferramenta online para bloqueio ou permissão de IPs específicos desejados pela CONTRATANTE;

2.5.18. A plataforma deve possuir linguagem de programação intuitiva e simples para a construção de políticas de segurança mais complexas.

2.5.19. A plataforma deve conter mecanismos de proteção e mecanismos de alertas tais como:

2.5.19.1. Proteção antibot;

2.5.19.2. Proteção contra ataques na Web de dia zero;

2.5.19.3. TCO reduzido com mais baixos falsos positivos;

2.5.19.4. Dispositivo de prevenção de DDoS;

2.5.19.5. Comportamento Profundo Baseado em Intenção Análise;

2.5.19.6. Cobertura total das ameaças automatizadas da OWASP;

2.5.19.7. Proteger todos os canais: aplicativos Web e móveis, APIs;

2.5.19.8. Este tipo de proteção não deve fornecer proteção baseada apenas em assinaturas, mas também possuir modelos de segurança positivos e/ou detecção de anomalia.

2.5.20. A plataforma deve realizar a análise dos IPs requisitantes protegendo as aplicações de serem acessadas pelas seguintes origens: rede TOR, proxies anônimos e endereços IP de baixa reputação.

2.5.21. A plataforma deve proteger as contas de usuários das aplicações contra ataques.

2.5.22. A solução deverá integrar-se com a maioria dos principais sistemas de Gerenciamento de Informações e Eventos de Segurança (SIEM). Deverá conter com a possibilidade de exportar eventos como mensagens syslog, formato Common Event Format (CEF) e formato JSON, permitindo pesquisas para rápidas respostas a possíveis incidentes e intuitivamente indexados.

2.5.23. A solução contratada, deverá permitir a integração, manual ou automática, de regras resultantes das análises de vulnerabilidade periódicas a serem executadas de acordo com a frequência quando houver necessidade de análise das URLs por parte da CONTRANTE.

2.5.24. A plataforma de posse dos resultados do scanner de vulnerabilidade, deverá aplicar “patches virtuais” nas aplicações vulneráveis, de forma a protegê-la de ataques.

2.5.25. Deverá contemplar o monitoramento do ambiente onde a solução de WAF estiver sendo executada, evitando perdas de performance que possam prejudicar o serviço contratado.

2.5.26. Dentre as possibilidades de chamados técnicos devem estar contemplados: apoio a configurações, criação de regras, refinamento de regras, customização de relatórios e resolução de problemas;

2.5.27. A CONTRATADA deverá licenciar e disponibilizar recursos adequados, conforme detalhamento:

2.5.27.1. Proteção de quantidade de URLs determinada determinado para atender a CONTRATANTE na sua necessidade atual a ser levantado pela CONTRATADA;

2.5.27.2. A vazão de tráfego (throughput) mínima do serviço será de 100 (cem) Mbps.

## 2.6. Descrição Mínima das Atividades de Administração de Dados

2.6.1. A administração de dados deverá englobar os Sistemas Gerenciadores de Banco de Dados (SGBDs), bem como quaisquer componentes ou produtos correlatos mencionados no item específico que trata dos componentes de banco de dados.

2.6.2. A CONTRATADA executará a restauração de bases de dados, a partir de um backup especificado ou a partir de qualquer dos servidores hospedados no data center (copy only), entre os diferentes servidores da solução, em até 24h corridas após a solicitação da CONTRATANTE. Exemplos: restauração do último backup full do banco ABC no servidor B1 para o banco ABC no servidor B2; cópia do banco ABC do servidor B3 para o banco ABC no servidor B4. Em caso de urgência, devidamente justificada pela CONTRATANTE, a CONTRATADA deverá atender em até 4h.

2.6.3. A restauração mencionada no item anterior, quando feita em ambiente distinto e sobrepondo bases de dados previamente existentes, deverá respeitar as configurações e opções do ambiente de destino (perfis, permissões, *recovery model*, etc.). A CONTRATANTE é responsável por determinar o local de destino da restauração da base de dados solicitada.

2.6.4. Emitir alertas de monitoração das bases de dados, via e-mail e/ou SMS, para os destinatários informados pela CONTRATANTE, sempre que ocorrerem eventos de interesse desta. A definição dos eventos que irão gerar tais alertas será feita durante a execução do ambiente após a migração, conforme especificado neste documento. Entre os eventos a serem monitorados estão as falhas de jobs, AlwaysOn check health e os erros dos eventos erros do log, Estes eventos serão selecionados a partir dos eventos gerados automaticamente pelos Componentes de Banco de Dados.

2.6.5. Subsidiar a CONTRATANTE quanto à ativação, instalação, funcionamento, melhoria e atualização dos diversos Componentes de Banco de Dados existentes no ambiente da CONTRATANTE.

2.6.6. Prover migração de dados entre Componentes de Banco de Dados, conforme solicitação e planejamento estabelecidos pela CONTRATANTE.

2.6.7. Criar os ambientes necessários aos Componentes de Banco de Dados, de acordo com boas práticas de mercado, apoiando a CONTRATANTE na elaboração de Normas Internas.

2.6.8. Seguir processos do ITIL, nas disciplinas de gerenciamento de incidentes, problemas, configuração, mudança e liberação.

2.6.9. Instalar e configurar Componentes de Banco de Dados.

2.6.10. Manter os Componentes de Banco de Dados nos diferentes ambientes (produção, homologação, desenvolvimento), garantindo a sua estabilidade, confiabilidade, desempenho e disponibilidade.

2.6.11. Apoiar a equipe técnica da CONTRATANTE na elaboração das políticas de replicação e de backup dos dados e configurações armazenados em Bancos de Dados (BD), implantando os agentes e realizando as configurações necessárias para o funcionamento correto das soluções, caso necessário.

2.6.12. Configurar os parâmetros necessários para o correto funcionamento, utilizando todos os recursos disponíveis nos servidores utilizados pelos Componentes de Banco de Dados.

2.6.13. Administrar e configurar os Componentes de Banco de Dados seguindo as práticas de segurança, conforme determinação da CONTRATANTE.

2.6.14. Monitorar o desempenho, capacidade e continuidade dos Componentes de Banco de Dados de forma a detectar e corrigir eventuais problemas.

2.6.15. Gerar relatórios sobre a disponibilidade do serviço e possíveis pontos de falha, inclusive prevendo o crescimento das bases e quando deverá ser alocado mais espaço para tais dados.

- 2.6.16. Implantar soluções de alta disponibilidade, cluster, balanceamento de carga, migração de dados e tolerância a falhas para os serviços críticos.
- 2.6.17. Manter documentação completa da instalação e funcionamento dos Componentes de Banco de Dados, inclusive topologias dos nós de clusters, replicação, *linked servers* e sistemas de balanceamento de carga.
- 2.6.18. Aplicar patches de correção e/ou atualização necessários para redução no risco de falhas e vulnerabilidades e disponibilização de melhorias nos Componentes de Banco de Dados.
- 2.6.19. Atender solicitações e requisições da equipe técnica da CONTRATANTE presencialmente, por e-mail, mensagem instantânea e/ou telefone.
- 2.6.20. Informar DBA ou grupo de DBA's de plantão, para acesso direto por parte da equipe técnica da CONTRATANTE em caso de emergências, sem prejuízo da abertura de chamado para registro do incidente / requisição de serviço.
- 2.6.21. Subsidiar a equipe técnica da CONTRATANTE na elaboração de projetos para a melhoria dos serviços da área.
- 2.6.22. Elaborar relatórios técnicos que subsidiem a CONTRATANTE no gerenciamento de contratos de serviços de TI e homologação de equipamentos e softwares.
- 2.6.23. Coordenar a criação, verificação, atualização e implementação dos scripts de solução de problemas na área de Administração de Dados.
- 2.6.24. Produzir, conferir e executar scripts nos SGBDs e demais Componentes de Banco de Dados – SQL, MDX, DAX, shell scripts, DDL, DCL ou DML necessários ao funcionamento e implantação de funcionalidades aos bancos de dados, quando solicitado.
- 2.6.25. Elaborar auditorias de dados, consultas às bases de logs de transações, relatórios diversos que não estejam implantados nas aplicações existentes.
- 2.6.26. Dar suporte à Equipe de Tratamento de Incidentes de Redes – ETIR.
- 2.6.27. A delegação da administração dos Componentes de Banco de Dados por parte da CONTRATANTE não ensejará perda dos direitos administrativos sobre os sistemas em questão. Caso a CONTRATADA deseje se resguardar de possíveis falhas operacionais ocasionadas por ação da equipe técnica da CONTRATANTE, esta poderá implantar os métodos de rastreabilidade que julgar necessários, desde que sejam previamente aprovados por ambas as partes. Da mesma forma, a CONTRATANTE se resguarda o direito de auditoria nas operações realizadas em seus ativos.

## 2.7. Descrição Mínima do Ambiente Específico de Banco de Dados

- 2.7.1. A versão de SGBD atualmente em uso é o SQL Server Enterprise Edition 2017.
- 2.7.2. As licenças para execução de todos os SGBDs e demais Componentes de Banco de Dados serão de responsabilidade da CONTRATADA, podendo a CONTRATANTE solicitar o upgrade para a versão mais recente sem ônus adicional para a CONTRATANTE.
- 2.7.3. Entende-se por Componentes de Banco de Dados quaisquer *features* que venham a ser instaladas e inclusas no licenciamento do SQL Server Enterprise Edition com *Software Assurance*, ou a distribuição que venha a sucedê-la, tais como: SQL Server Integration Services, SQL Server Analysis Services, SQL Server Reporting Services, SQL Server Data Quality Services, SQL Server Master Data Services, etc.
- 2.7.4. A CONTRATADA deverá prover ambientes dedicados para os Componentes de Banco de Dados em produção, homologação e desenvolvimento. Tais ambientes poderão sofrer alterações ao longo do contrato, observados os limites máximos de utilização de recursos computacionais e a distribuição de recursos e serviços que garanta a melhor performance e disponibilidade do ambiente.
- 2.7.5. A configuração inicial dos ambientes consistirá no mínimo dos seguintes servidores de aplicação:
- 2.7.5.1. Produção – Operacional.
- 2.7.5.2. Produção – Dados Gerenciais.
- 2.7.5.3. Homologação.
- 2.7.5.4. Desenvolvimento.

2.7.6. A instalação dos Componentes de Banco de Dados em todos os servidores e sua configuração, de acordo com parâmetros fornecidos pela CONTRATANTE, será de responsabilidade da CONTRATADA.

2.7.7. A atualização de *major releases* dos Componentes de Banco de Dados (por exemplo, da versão 2017 para a versão 2022 ou outra que venha a sucedê-la) é de responsabilidade da CONTRATADA e deverá ser realizada em até 6 meses após o lançamento de novas versões, ressalvada a hipótese da CONTRANTE precisar manter a versão anterior em uso e desde que tal versão esteja ainda no período de suporte do fabricante.

## 2.8. Descrição Mínima dos Volumes de Armazenamento de Blocos

2.8.1. Deverá ser baseado em discos de estado sólido (SSD), com conexões NVMe, fornecendo no mínimo 2.000 (dois mil) IOPS (Input / Output Operations per Second) para cada 1024 GB de armazenamento.

2.8.2. Serviço para utilização de volume de armazenamento block-level. Os equipamentos do storage devem suportar acréscimos de volume de armazenamento de no mínimo 300TB.

2.8.3. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo Sistema Operacional como um dispositivo físico e local.

2.8.4. O serviço deve permitir a definição de nomes ou identificadores – (Ids) de volumes de armazenamento.

2.8.5. O serviço deve permitir a expansão ou redução do volume do bloco conforme demanda da CONTRATANTE.

2.8.6. O custo do serviço de utilizará a métrica de volume em 1000 GB dos blocos disponibilizados. A CONTRATADA fornecerá em relatório mensal, além do volume disponibilizado, o volume efetivamente consumido pela CONTRATANTE associado a cada servidor virtual.

## 2.9. Requisitos Mínimos do Serviço de Backup e da Restauração de Dados

2.9.1. O serviço de backup garantirá que as informações da CONTRATANTE estejam disponíveis para recuperação no caso de remoção acidental de arquivos, erros, problemas, falhas, desastres ou outras ações não planejadas.

2.9.2. A CONTRATADA, deverá utilizar discos (HDD ou SSD) para realização das cópias. Os dados do serviço de backup deverão ser armazenados em ambiente separado dos dados originais, considerando que a infraestrutura de backup estará em site secundário diferente do site de produção (principal).

2.9.3. O custo do serviço de backup utilizará a métrica de volume mensal em 1000 GB dos dados originais salvaguardados (área protegida). O volume de dados protegidos deve ser informado em relatório mensal entregue à CONTRATANTE.

2.9.4. Os serviços devem prover algoritmo de criptografia seguro, como AES 256 ou equivalente, conforme padrão internacional reconhecidamente aceito.

2.9.5. O serviço de backup deverá permitir definir o período de retenção de acordo com a seguinte frequência::

2.9.5.1. diária: incremental ou diferencial com retenção mínima de 1 mês;

2.9.5.2. semanal: completo (full) com retenção mínima de 1 mês;

2.9.5.3. mensal: completo (full) com retenção mínima de 6 meses.

2.9.6. O serviço de backup deverá disponibilizar registros (logs) dos acessos aos dados copiados da CONTRATANTE.

2.9.7. O serviço de backup deverá permitir a exclusão de tipos específicos de arquivos, por exemplo, arquivos temporários.

2.9.8. O serviço deverá possuir compatibilidade, no mínimo, para backup dos sistemas operacionais Windows Server e Linux.

2.9.9. O serviço deverá possibilitar backup dos gerenciadores de bancos de dados SQL Server, MariaDB e Postgresql, bem como das máquinas virtuais, do armazenamento em blocos SSD e dos diretórios do container de objetos MinIO.

2.9.10. O serviço de backup deverá possibilitar notificação via e-mail do status das cópias realizadas.

2.9.11. A CONTRATADA deverá seguir as políticas de confidencialidade e sigilo definidas pela CONTRATANTE.



2.9.12. A CONTRATANTE poderá solicitar, sempre que necessário, e sem qualquer ônus adicional, a restauração da cópia de segurança de qualquer ambiente ou componentes de ambiente.

2.9.13. Cabe à CONTRATANTE estabelecer a forma, a seleção de itens e a frequência da restauração das cópia de segurança. Todos os testes de restauração serão realizados sem ônus adicional para a CONTRATANTE.

2.9.14. Para realização da funcionalidade backup e restore, a CONTRATADA deverá disponibilizar solução completa, com todos os recursos necessários para executar as rotinas da CONTRATANTE, sendo que a solução de backup deverá estar preparada para geração automática de imagens das máquinas virtuais (snapshots), a critério da CONTRATANTE.

2.9.15. O serviço de backup deverá ser fornecido com as seguintes características:

2.9.15.1. Proteção anti-ransomware;

2.9.15.2. Proteção anti-malware baseada em autoaprendizagem;

2.9.15.3. Avaliação de vulnerabilidades e failover de teste.

2.9.15.4. Realização testes semestrais de Disaster Recovery (DR) através de um ambiente isolado (ambiente bolha).

2.9.16. As solicitações de exclusões e inclusões de novas áreas de armazenamento nas cópias de segurança deverão ser efetivamente operacionalizadas pela CONTRATADA, em um prazo máximo de 24 (vinte e quatro) horas.

2.9.17. O serviço de backup permitirá à CONTRATANTE acessar e copiar seus dados em formato padrão de mercado, por, no mínimo, 6 (seis) meses após o encerramento da prestação dos serviços. Após o transcurso deste prazo, a CONTRATADA deverá garantir a exclusão imediata, segura e definitiva da integralidade dos dados guardados no serviço de backup.

## 2.10. Gerenciamento dos Sistemas Operacionais

2.10.1. A CONTRATADA é responsável por:

2.10.1.1. Aplicação de atualizações e correções de segurança (patches).

2.10.1.2. Suporte técnico para instalação e configuração de software.

2.10.1.3. Suporte técnico para instalação e configuração de funcionalidades (features) do sistema operacional.

2.10.1.4. Criação de Requisição de Certificado SSL (CSR – Certificate Signing Request).

2.10.1.5. Instalação de certificado SSL. O fornecimento dos certificados será de responsabilidade da CONTRATANTE.

## 2.11. Atualizações de Software

2.11.1. A CONTRATADA deverá acompanhar as notas divulgadas pelos fornecedores dos softwares por ela administrados de modo a realizar a correção de falhas e vulnerabilidades de forma eficaz e tempestiva.

2.11.2. O processo de atualização, quando necessário, deve ser executado em etapas, com a instalação sucessiva nos ambientes de desenvolvimento, homologação e produção e com prévia notificação/anuência da CONTRATANTE.

2.11.3. Qualquer atualização crítica ou de segurança deve ser aplicada em até 30 dias após a sua divulgação. Casos excepcionais, para os quais haja a recomendação de aplicação de correções em prazos mais curtos, deverão ser analisados pela CONTRATADA e submetidos à aprovação da CONTRATANTE.

## 2.12. Plataforma de virtualização

2.12.1. A plataforma de virtualização a ser utilizada deverá possuir as seguintes características mínimas:

2.12.1.1. Deverá utilizar preferencialmente o virtualizador Microsoft Hyper-V, em face da elevada utilização de máquinas virtuais Windows Server e SQL Server na presente contratação, podendo ser utilizado alternativamente o virtualizador VMWare. A utilização de virtualizador diverso dos citados dependerá de prévia e expressa autorização da CONTRATANTE.

2.12.1.2. Criar máquinas virtuais em equipamentos físicos dotados de processadores baseados na tecnologia X86\_64 ou compatíveis.

2.12.1.3. Isolar totalmente as máquinas virtuais, impedindo a comunicação entre elas a não ser pelo ambiente de rede em que serão inseridas.

2.12.1.4. Suportar máquinas virtuais coexistindo no mesmo equipamento com quaisquer dos sistemas operacionais citados neste documento.

2.12.1.5. Possibilitar a instalação em servidor físico sem disco físico local, podendo ser iniciado através de uma SAN (Storage Area Network) utilizando o conceito de “diskless”.

2.12.1.6. Suportar extensão do tamanho do disco virtual enquanto a máquina virtual permanece ligada.

2.12.1.7. Permitir a formação de um ou mais clusters, com emprego de dois ou mais hosts físicos para manutenção de disponibilidade.

2.12.1.8. Permitir a criação de switches virtuais locais em cada host físico ou distribuído pelo cluster, e que suportem VLANs.

2.12.1.9. Acessar a SAN (“Storage Area Network”) por mais de um caminho (“multipath”) e tolerante a falha (“failover”).

2.12.1.10. Ter sistema de arquivos que permita ser configurado em “storage” compartilhado, onde mais de um servidor físico consiga acessar o mesmo compartilhamento simultaneamente.

2.12.1.11. Criar ambiente de alta disponibilidade, por meio de “cluster” ou tecnologia superior, entre as máquinas virtuais, mesmo que estas estejam em servidores físicos diferentes.

2.12.1.12. Permitir o balanceamento de carga gerado pelas máquinas virtuais com a movimentação destas máquinas entre os servidores físicos sem causar indisponibilidade do serviço.

2.12.1.13. Permitir integração com o software de backup fornecido pela CONTRATADA para que seja possível o restore completo das imagens das máquinas virtuais e de arquivos dentro destas imagens.

2.12.1.14. Permitir integração do ambiente de virtualização com os principais fornecedores de antivírus do mercado (Mcafee, Symantec, Trend, etc.).

2.12.1.15. Emitir alertas parametrizáveis por e-mail e traps SNMP.

2.12.1.16. Possibilitar a integração com o serviço de diretório Microsoft Active Directory sem a necessidade de alterar o esquema do serviço de diretório.

2.12.1.17. Possibilitar monitorar o uso dos recursos, como máquinas e dispositivos de rede virtuais, inclusive identificar recursos ociosos.

2.12.1.18. Possibilitar o cadastramento dos colaboradores da CONTRATANTE para consultar o ambiente de computação disponibilizada pela CONTRATADA.

2.12.1.19. Todas as operações realizadas pelos usuários da CONTRATANTE no gerenciamento dos recursos devem ser registrados e passíveis de auditoria.

2.12.2. Deverá ser disponibilizado acesso de leitura para que a equipe técnica da CONTRATANTE tenha visibilidade da console de virtualização a qualquer tempo, além de relatórios gerenciais mensais de disponibilidade para a aferição da prestação de serviços.

2.12.2.1. A Solução deve comportar armazenamento de logs de auditoria das atividades administrativas por pelo menos 30 dias

## **2.13. Suporte Técnico da Contratada**

2.13.1. A CONTRATADA deverá prestar serviços de configuração e administração dos recursos computacionais, alocando profissionais qualificados tecnicamente para operar os recursos contratados, seguindo as regras de negócio da CONTRATANTE.

2.13.2. A CONTRATADA deverá prover ponto único de contato, serviço centralizado destinado à recepção de todas as demandas da CONTRATANTE e abertura dos respectivos chamados, acessível por meio de canais telefone, email e Portal Web, envolvendo todo o objeto, incluindo os serviços subcontratados. A CONTRATADA irá permitir o cadastro de no mínimo 8 (oito) usuários da CONTRANTE no Portal Web para acompanhamento dos chamados técnicos. Sempre que possível, deverá haver integração entre o sistema de ITIL da CONTRATANTE (Sysaid) e o sistema correspondente da CONTRATADA.

2.13.3. Será designado no mínimo um funcionário da CONTRATADA para providenciar o andamento e resolução das demandas da CONTRATANTE.

2.13.4. O serviço de suporte técnico deverá ser prestado em regime integral, ou seja, disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, em linguagem português brasileiro.

2.13.5. O suporte técnico será prestado sem qualquer ônus adicional para a CONTRATANTE mesmo quando for necessária a atualização de equipamentos, o deslocamento e a estada de técnicos da CONTRATADA ou qualquer outro tipo de serviço necessário para garantir o cumprimento dos níveis mínimos de serviço exigidos.

2.13.6. O serviço de suporte técnico deverá ser solicitado pela equipe de TI da CONTRATANTE através da abertura de chamado junto à CONTRATADA, e os chamados deverão ser classificados, a critério da equipe de TI da CONTRATANTE, de acordo com as seguintes categorias de severidade de incidentes:

Descrição de Severidade - INCIDENTES		
1	Crítico	Sistema em produção parado ou inoperante, e não há meios de contornar a falha. Número significativo de usuários afetados, podendo causar riscos financeiros, regulatórios, de segurança ou de reputação. (Ex.: perda total de conectividade do ambiente ou falha massiva do Backbone).
2	Alto	Erro ou problema que afete o negócio significativamente, mas com solução de contorno possível. (ex.: perda parcial de conectividade e/ou funcionalidade etc.)
3	Médio	Perda parcial ou limitada de funcionalidade não-crítica, com os serviços fundamentais disponíveis (ainda que por solução de contorno).  Problema ou inconsistência que não interfira diretamente nas tarefas diárias.
4	Baixo	Problemas que afetem um único usuário ou pequeno grupo, esclarecimentos da documentação, dúvidas técnicas etc.

2.13.7. Na abertura dos chamados será definida a categoria de severidade dos incidentes (crítico, alto, médio e baixo) pela CONTRATANTE e deverá ser disponibilizado sistema Web para acompanhamento destes.

2.13.8. A contagem do prazo de solução definitiva de cada chamado iniciar-se-á a partir da data/hora da abertura do chamado, em um dos canais de atendimento disponibilizados pela CONTRATADA, até a resolução definitiva do problema e o aceite pela equipe de TI da CONTRATANTE.

Prazo de Solução Definitiva (em horas corridas a partir da abertura)			
Crítico	Alto	Médio	Baixo
4 (quatro)	8 (oito)	24 (vinte e quatro)	48 (quarenta e oito)

2.13.9. Em relação às solicitações de Serviços, os prazos para atendimentos são os que se seguem:

Descrição do Serviço		Prazo máximo (em dias úteis)
1	Autorizar/alterar/excluir acesso de usuário a VPN (client-to-site)	1
2	Configuração de VPN Site-to-Site	2
3	Criação/Modificação de Regra de Firewall / WAF	1
4	Configuração de Sub-rede/VLAN	1
5	Configurar IP público	1
6	Configuração de Domínio de DNS	1
7	Criação/Alteração de Recursos e configuração/Exclusão de Máquina Virtual	1
8	Serviço de análise e melhoria de desempenho (tuning) de componentes de banco de dados	2
9	Criação de Requisição de Assinatura de Certificado (CSR)	1
10	Instalação de Certificado SSL	2
11	Restauração de Backup	1
12	Restauração de bancos de dados (exceto as situações de incidente, que seguirão os prazos previstos no item próprio anteriormente citado)	1
13	Criação/alteração/exclusão de usuário	1
14	Criação de snapshot de VM	1
15	Criação/alteração/exclusão de perfil de webfilter	1
16	Configuração de antispam	1

17	Solicitação de relatórios previstos no escopo deste Termo de Referência	2
18	Outras solicitações de serviço no escopo deste Termo de Referência	2

2.13.10. A contratada deverá emitir mensalmente, até o 5º dia útil, relatório dos chamados abertos pela contratante e encerrados no mês anterior, no qual constem minimamente os seguintes dados:

- 2.13.10.1. Identificador do chamado;
- 2.13.10.2. Usuário autor do chamado;
- 2.13.10.3. Teor resumido do chamado;
- 2.13.10.4. Data/hora de abertura;
- 2.13.10.5. Data/hora de encerramento;
- 2.13.10.6. Severidade;
- 2.13.10.7. Prazo previsto para solução;
- 2.13.10.8. Prazo da efetiva solução;
- 2.13.10.9. Se houve ou não violação do NMS.

2.13.11. A contratada emitirá, no mesmo prazo e mesmos dados do item anterior, relatório em que constem os chamados pendentes de atendimento abertos pela contratante até o final do mês anterior

#### 2.14. Link de Acesso à Internet

2.14.1. A CONTRATADA deverá disponibilizar link de acesso do data center à internet com banda garantida de 2 Gbps, assim entendida como o valor efetivo mínimo de banda entregue à CONTRATANTE, por links simétricos, ou seja, com velocidades mínimas iguais de download e upload em disponibilidade mínima de 99,741%.

2.14.2. Nos custos deste item estão inclusos os serviços de Anti-DDOS conforme descrito a seguir neste documento.

2.14.3. O serviço deve contemplar a capacidade de administração de alto tráfego a ser provido pelos links de comunicação e suportar classes de serviços e IEEE 802.1p, e ainda, permitir a configuração dos parâmetros de qualidade (QoS).

2.14.4. A CONTRATADA deverá responder pela elaboração e manutenção do mapa de endereçamento IP utilizado nas redes IP de acesso. Tais endereços devem ser plenamente compatíveis com o plano de endereçamento das redes LAN.

2.14.5. A CONTRATADA deverá prestar suporte à empresa responsável pela conectividade das unidades da CONTRATANTE à internet e ao data center. Esta conectividade poderá ser realizada através de VPN site-to-site com firewall da CONTRATADA ou através de appliance virtual instalado no ambiente de data center.

2.14.6. O máximo de latência admitido pela CONTRATANTE no Serviço de comunicação de dados, fim-a-fim, entre a sede da Autarquia e o ambiente de hospedagem da CONTRATADA é de 10 ms (dez milissegundos). A latência será considerada como o tempo médio que os pacotes IP levam para ir de um ponto a outro e retornar à origem.

2.14.7. A CONTRATADA deverá entregar, até o 5º dia útil do mês seguinte ao período de apuração, o relatório de latência com as verificações do percentual de pacotes acima do limite de latência.

2.14.8. A CONTRATANTE poderá solicitar por aditivos contratuais o aumento do link de tráfego de saída do data center à internet, no qual ocorrerá de forma simultânea e proporcional o aumento no custo de serviço de firewall conforme especificado na planilha de custos.

2.14.9. O máximo de perda de pacotes admitido pela CONTRATANTE para o link de acesso do data center à internet é de 1% (um por cento). índice que será aferido pela CONTRATADA da seguinte forma: até o 5º dia útil do mês seguinte ao período de apuração, a CONTRATADA deverá entregar o Relatório de Perda de Pacotes com as verificações do percentual de pacotes perdidos.

## 2.15. Serviço Anti-DDOS

2.15.1. O serviço de proteção Anti-DDOS (Distributed Denial of Service) deverá ter capacidade de detectar e mitigar, de forma automática, todos e quaisquer ataques que façam uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes:

2.15.1.1. ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

2.15.1.2. ataques à pilha TCP, incluindo mau uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

2.15.1.3. ataques que utilizam fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

2.15.1.4. ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

2.15.1.5. ataques denominados Comand-and-Control e Remote Access Trojans;

2.15.1.6. (RATs).

2.15.2. O serviço deverá ter capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

2.15.3. O serviço deverá manter lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro.

2.15.4. O serviço deverá manter atualizadas as “assinaturas/impressões digitais” de ataques disponibilizados pelo fabricante da solução de detecção, monitoramento e mitigação de ataques.

2.15.5. A CONTRATADA (ou SUBCONTRATADA) deverá possuir, no mínimo, 1 (um) centro de limpeza próprio nacional, 1 (um) centro de limpeza próprio internacional, ambos com capacidade de mitigação suficiente para atender às bandas garantidas estabelecidas neste documento, incluídos os possíveis aumentos contratuais estabelecidos.

2.15.6. O serviço de mitigação deverá ser prestado sem limitação de tempo de duração do ataque e sem limitação da quantidade de eventos de ataque.

2.15.7. O serviço deverá garantir a entrega de tráfego legítimo compatível com a capacidade total do enlace vigente.

2.15.8. As funcionalidades de monitoramento, detecção e mitigação de ataques deverão ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

2.15.9. A mitigação de um eventual ataque DDoS deverá estar plenamente operacional, atuando no enlace Internet sob ataque, em até 15 minutos após a detecção.

2.15.10. Em caso de ocorrência de ataque que não seja plenamente mitigado pela solução, a CONTRATADA deverá notificar de imediato a equipe técnica da CONTRATANTE.

2.15.11. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio (deviation) de tráfego suspeito para o Centro de Mitigação na infraestrutura da CONTRATADA, através de alterações do plano de roteamento, de forma transparente para a CONTRATANTE, com encaminhamento (re injection) do tráfego limpo para a rede da CONTRATANTE.

2.15.12. O desvio de tráfego suspeito para o Centro de Mitigação somente deverá ocorrer em caso de detecção de ataques. Ou seja, o tráfego da CONTRATANTE não deverá ser desviado em situação de operação normal.

2.15.13. O tráfego suspeito deverá ser sempre desviado para o Centro de Mitigação mais próximo possível da origem dos ataques, seja nacional ou internacional.

2.15.14. Deverá ser possível realizar o desvio, para o Centro de Mitigação, somente do tráfego dirigido para o (s) IP(s) sob suspeita de ataque.

2.15.15. No procedimento de mitigação de ataques fica proibido o encaminhamento do tráfego para análise e limpeza fora do território brasileiro, exceto se o tráfego de origem for proveniente do exterior, caso em que será permitido o encaminhamento do mesmo para um centro de mitigação fora do território nacional disponibilizado pela CONTRATADA.

2.15.16. A mitigação deverá ocorrer dentro da própria rede da CONTRATADA ou da subcontratada conforme o caso.

2.15.17. O serviço Anti DDOS poderá ser subcontratado seguindo as mesmas regras de subcontratação estabelecidas para o serviço de conectividade/enlace de dados.

## 2.16. Migração de Ambiente

2.16.1. A execução dos serviços de migração será iniciada na data de início da vigência do Contrato, na forma que se segue.

CRONOGRAMA DA MIGRAÇÃO DO AMBIENTE		
ETAPAS	Prazos Previstos	
D: data constante da Ordem de Serviço.	Início	Fim
1 - Instalação de link provisório ponto a ponto dedicado de 10Gbps (ou superior) entre o data center da atual CONTRATADA (Telefonica Brasil S/A) e o data center da nova CONTRATADA. Provisionamento do ambiente da CONTRADA.	D	D + 30
2 - 2ª. Etapa – Replicação do Ambiente Operacional da CONTRATANTE no Ambiente da nova CONTRATADA utilizando a tecnologia de Data Center Replication - DR	D	D + 80
2.1 - Clonagem das máquinas virtuais e banco de dados com importação das máquinas para o novo ambiente e conexão com os recursos de rede. Migração dos registros de DNS e Regras de Firewall e VLAN's para o novo ambiente.	D	D + 80
2.2 - Testes de ambiente pela CONTRATANTE e CONTRATADA.	D	D + 80
3 - 3ª. Etapa - Homologação do Ambiente Operacional da CONTRATANTE no Centro de Dados da CONTRATADA. Ruptura do link de serviços junto à Telefônica Brasil S/A.	D	D + 90

2.16.2. A CONTRATADA deverá seguir também as diretrizes constantes dos anexos deste Termo de Referência para a migração de data center.

2.16.3. A estratégia a ser adotada pela CONTRATADA para migração do ambiente é o do tipo Rehost ("Lift and Shift") com comunicação entre data centers através de link provisório dedicado ponto a ponto de 10 Gbps (no mínimo) em alta disponibilidade a ser instalado pela CONTRATADA (Golden Jumper).

2.16.4. O data center da atual CONTRATADA Telefônica Brasil S/A está localizado no seguinte endereço: Av. Marcos Penteado de Ulhoa Rodrigues, 1690 - Santana do Parnaíba – SP (acessível pela saída 23-A da Rodovia Presidente Castelo Branco).

2.16.5. A atividade acima será supervisionada por servidores da CONTRATANTE que também será responsável pelas autorizações de acesso ao ambiente da Telefônica Brasil S/A para as replicações citadas.

2.16.6. A Migração total dos dados, sistemas, e demais serviços da CONTRATANTE deverá ser finalizada em até 90 (noventa) dias a partir da data constante da Ordem de Serviço emitida para este fim.

2.16.7. Durante a migração do ambiente propriamente dita, a CONTRATADA deverá realizar as seguintes atividades.

2.16.7.1. Replicação de todos os dados do ambiente de TIC e de todos os subsistemas de armazenamento de dados da CONTRATANTE, hospedados na Telefônica Brasil S/A, para o data center da CONTRATADA.

2.16.7.2. Migração das regras de firewall que atualmente encontram-se implantados na Telefônica Brasil S/A, no que couber, para os firewalls da licitante vencedora do certame. As regras serão disponibilizadas em arquivo de configuração nativo da Telefônica Brasil S/A e caberá à CONTRATADA importá-las diretamente em seu ambiente, ou fazer a conversão para importação em ambiente diferente.

2.16.8. O ambiente atual da CONTRATANTE é composto por servidores virtuais e bancos de dados, sob o virtualizador VMWare. Consta dos anexos a relação de servidores com a respectiva volumetria.

### 3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A presente contratação justifica-se pela necessidade da serviço de hospedagem de recursos de TIC para atender às demandas da CONTRATANTE, atualmente sob o Contrato nº 02/2020 firmado junto à Telefônica Brasil S/A no processo SEI /SUSEP nº 15414.608821/2019-12.

3.2. Em face da atuação da Susep (fiscalizar a constituição, organização, funcionamento e operação das Sociedades Seguradoras, de Capitalização, Entidades de Previdência Aberta e Resseguradores, zelar pela defesa do interesse dos consumidores junto ao mercado supervisionado, monitorar a estabilidade, liquidez e solvência deste mesmo mercado) configura-se como grande desafio da Coordenação de Sustentação de Serviços de Tecnologia - COSIT estruturar adequadamente informações e dados para compor a visão estratégica da organização, buscando alinhar a missão e os objetivos da instituição com os objetivos estratégicos desta mesma COSIT.

3.3. Com efeito, a demanda de processamento da Autarquia tem aumentado significativamente nos últimos anos e, assim como acontece no mercado, novos serviços são criados para atender às necessidades internas da Administração bem como para as entidades supervisionadas. Para suportar este crescimento, a área de Tecnologia de Informação e Comunicações (TIC) também precisou evoluir, aumentando a quantidade de equipamentos e sistemas nesta Instituição. Com isso, aumentou também a complexidade e, conseqüentemente, a responsabilidade por manter todo ambiente operacional e os sistemas/serviços disponíveis.

3.4. A Susep concluiu em outubro de 2023 o projeto de migração da integralidade dos recursos computacionais para o data center da Telefônica Brasil S/A. Adiciona-se que desde a pandemia de COVID-19, a maior parte dos trabalhos realizados pela Autarquia (superior a 95%) são oriundos de trabalho em home office e que o Contrato atual foi elaborado em 2019, onde havia um cenário completamente diverso do presente onde havia 100% dos trabalhos realizados no regime presencial.

3.5. Houve ainda no exercício de 2023 a entrada em funcionamento da fase 1 do projeto SRO - Sistema de Registro de Operação, que vem agregando expressivo quantitativo de dados dos mercados supervisionados em ambiente de data center da Susep, o que vem demandando aumento elavado de recursos computacionais, tráfego de dados e requisitos de segurança da informação.

3.6. De forma a atender a nova demanda e desafios da Autarquia, foram estabelecidas as seguintes premissas nesta contratação:



3.6.1. os recursos providos no data center da atual Contratada, máquinas virtuais e armazenamento, foram contabilizados e descritos no anexo III - Planilha de Volumetria Atual. Estes recursos estão refletidos na Planilha de Custos no campo de estimativa inicial.

3.6.2. a estes campos foi aplicada a metrica de crescimento estabelecida no Estudo Técnico Preliminar com a expectativa de aumento baseada em método estatístico de regressão linear considerando-se o prazo total de 36 meses de contrato e possível prorrogação até 60 meses.

3.6.3. com respeito ao armazenamento HDD, foi considerado o aumento do uso atual adicionado do crescimento proveniente transferência dos dados do SRO - Sistema de Registros de Operações para a Susep, estimando-se aumento no serviço de armazenamento em HDD.

3.7. Com a nova contratação espera-se a prestação de serviço mais adequado à nova realidade da Susep, incluindo aumentos causados pelos novos projetos de supervisão de mercados bem como com a chegada de novos servidores em concurso previsto para o triênio 2024-2026.

3.8. Entre os benefícios da nova contratação estão:

3.8.1. Manter os serviços que fazem uso da infraestrutura de data center em funcionamento e com baixo risco;

3.8.2. Aumentar a redundância e resiliência dos serviços de infraestrutura de TIC, minimizando riscos;

3.8.3. Melhorar a segurança das informações armazenadas por meio de equipamentos modernos e seguros;

3.8.4. Prover a SUSEP de recursos tecnológicos e conhecimentos necessários à utilização de infraestrutura de data center.

3.8.5. Permitir a migração e prover funcionamento adequado aos ambientes já criados por meio do Contrato Susep nº 02/2020.

3.9. O objeto da contratação está alinhado com a Estratégia de Governo Digital 2024 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2024 da Superintendência de Seguros Privados - SUSEP, conforme demonstrado abaixo:

ALINHAMENTO AO PDTIC 2022-2024			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
IA#155	Contratar e Prorrogar serviços críticos de TIC	M#62	Manutenção de serviços críticos ao funcionamento da TI e da Susep

3.10. 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.

#### 4. REQUISITOS DA CONTRATAÇÃO

##### Requisitos de Negócio

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

4.1.1. Manter a disponibilidade, segurança e usabilidade dos serviços contratados;

4.1.2. Manter a resiliência e eficiência dos sistemas de informação da CONTRATANTE.

4.1.3. Os serviços de hospedagem em data center deverão ser prestados de modo parcialmente ou totalmente gerenciados conforme demandado pela CONTRATANTE.

- 4.1.4. A solução deverá prover serviços de gerenciamento, migração e suporte prestados por profissionais especializados, topologia automatizada e processos eficientes.

#### Requisitos de Capacitação

4.2. A CONTRATADA deverá fornecer treinamento online completo para os servidores e colaboradores da CONTRATANTE, sem ônus adicional, abordando os seguintes temas:

- 4.2.1. uso e acesso da plataforma de virtualização;
- 4.2.2. monitoração de todos os recursos do ambiente;
- 4.2.3. redes, VLAN, firewall e WAF;
- 4.2.4. abertura de chamados técnicos para todos os serviços previstos neste documento.

#### Requisitos Legais

4.3. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, 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 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Lei nº 10.520, de 17 de julho de 2001, Decreto 10.024, de 20 de setembro de 2019, e a outras legislações aplicáveis;

4.4. Deve-se observar, no que couber, os seguintes normativos:.

- 4.4.1. Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação;
- 4.4.2. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 e suas normas complementares - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
- 4.4.3. Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020 e suas normas complementares - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal
- 4.4.4. Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021 e suas normas complementares - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal
- 4.4.5. Norma Complementar nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012 - Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;
- 4.4.6. Norma Complementar nº 13/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, - Diretrizes para gestão de mudanças nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;
- 4.4.7. Norma Complementar nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014 - Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;
- 4.4.8. Instrução Normativa nº N 05/2021 GSI/PR - dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

4.5. Deve-se observar os seguintes padrões técnicos:

- 4.5.1. Tier 3 (EIA/TIA 942 ) ou TIER III (Tier Standard) - padrão de infraestrutura de telecomunicações para datacenters;
- 4.5.2. Service and Organization Controls 2 (SOC-2) - conformidade com os padrões de segurança da informação, por meio de auditoria anual SOC-2, conduzida por um auditor independente, com a apresentação do relatório de tipo II.

#### Requisitos de Manutenção

4.6. Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativas e evolutivas pela CONTRATADA, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades.

4.7. A CONTRATADA deve participar ativamente na identificação da causa raiz de problemas relacionados aos produtos entregues e serviços prestados.

4.8. A CONTRATADA deverá disponibilizar suporte técnico em nível corporativo com, no mínimo, as seguintes características:

4.8.1. Manter central de atendimento para abertura de chamados no regime 365x24x7 para atendimento dos chamados de suporte técnico. A central deverá ser acionada, preferencialmente, por meio de ligação gratuita ou ligação local no Rio de Janeiro/RJ, devendo a CONTRATADA disponibilizar abertura de chamados pela internet. O atendimento deverá ser realizado em língua portuguesa;

4.8.2. Disponibilização de orientações para provisionar seus recursos, seguindo as práticas recomendadas do provedor para a reduzir custos, aumentar o desempenho e a tolerância a falhas e melhorar a segurança;

4.8.3. Suporte a ambientes de produção, homologação e desenvolvimento;

4.8.4. Orientações relacionadas a arquitetura, projeto, design, operação e resolução de problemas.

#### Requisitos Temporais

4.9. Os serviços devem ser prestados no prazo máximo definido na Ordem de Serviço (OS) e estabelecidos neste Termo de Referência, a contar do recebimento da abertura da mesma, emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela CONTRATANTE. Os prazos constantes das OS's serão os estabelecido neste Termo de Referência,

4.10. 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.

4.11. Os prazos definidos neste Termo de Referência deverão ser estritamente observados sob pena da aplicação de sanções conforme previsto neste Termo de Referência, salvo ocorra expressa autorização fundamentada da CONTRATANTE.

#### Requisitos de Segurança e Privacidade

4.12. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da CONTRATANTE, estabelecida pela Deliberação SUSEP nº 171, de 19 de março de 2015, e

4.13. A CONTRATADA deverá assegurar durante a execução dos serviços a observância às disposições da Lei Geral de Proteção de Dados - LGPD - Lei 13.709, de 2018.

4.14. A CONTRATADA deverá adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações a serem tratadas no ambiente de data center.

4.15. A CONTRATADA deverá implementar medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade, prevenindo acesso não autorizado às informações.

4.16. A CONTRATADA deverá submeter-se aos procedimentos contidos nas normas de segurança corporativa da CONTRATANTE e da Administração Pública em todos os eventos em que for necessária a presença física ou virtual de seus prepostos e/ou funcionários.

4.17. A CONTRATADA deverá exigir dos seus empregados, quando em serviço presencial ou remoto para à CONTRATANTE, o uso obrigatório de identificação funcional.

4.18. A CONTRATADA não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado as informações de propriedade da CONTRATANTE.

4.19. A CONTRATADA deverá assinar o Termo de Compromisso, e seus funcionários alocados na prestação de serviços, o Termo de Ciência, conforme modelos anexos ao Termo de Referência:

4.20. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços da CONTRATADA ensejará a responsabilidade criminal, na forma da lei, sem prejuízo de outras providências nas demais esferas.

- 4.21. A Solução ofertada pela CONTRATADA deverá dispor de plano de comunicação de incidentes, devendo a CONTRATADA informar imediatamente à CONTRATANTE todos os incidentes de segurança da informação ou existência de vulnerabilidades do objeto da contratação, assim considerados os eventos não previstos ou não desejados, bem como qualquer violação das regras de sigilo estabelecidas que tenham ocorrido por sua ação ou omissão, independentemente de dolo, que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados da CONTRATANTE.
- 4.22. A CONTRATADA deverá possuir processo de análise e gestão de riscos de segurança de informação compatível aos dispositivos da Instrução Normativa nº 05/2021 GSI/PR
- 4.23. A CONTRATADA deverá observar no que lhe couber os dispositivos constantes da IN 05/2021 GSI/PR.
- 4.24. O processo de análise e gestão de riscos deve prever análises com periodicidade mínima trimestral, mantendo-se um plano de gestão de riscos atualizado e disponível à CONTRATANTE, contendo no mínimo: a descrição da metodologia utilizada, os riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes.
- 4.25. A CONTRATADA deve possuir e manter às informações disponíveis à CONTRATANTE:
- 4.25.1. O plano de continuidade, contendo as ações de recuperação de desastres e contingência de negócio;
  - 4.25.2. Os resultados dos testes trimestrais de avaliação dos mecanismos descritos no plano relacionados à disponibilidade dos dados e serviços em caso de interrupção;
  - 4.25.3. Plano de resposta à incidentes contendo os procedimentos relacionados à prevenção e resposta aos incidentes referentes aos serviços objeto deste Termo de Referência.
  - 4.25.4. Os resultados respostas a incidentes relacionados com os serviços.

#### Requisitos Sociais, Ambientais e Culturais

- 4.26. Os serviços devem estar aderentes às seguintes diretrizes sociais:
- 4.26.1. apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional da CONTRATANTE ou que ofenda o senso comum de moral e bons costumes;
  - 4.26.2. respeitar todos os servidores, funcionários e colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;
  - 4.26.3. atuar no estabelecimento da CONTRATANTE com urbanidade e cortesia.
- 4.27. Os serviços devem estar aderentes às seguintes diretrizes ambientais:
- 4.27.1. deverá entregar os documentos solicitados preferencialmente na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010);
  - 4.27.2. as configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos;
  - 4.27.3. utilizar de forma eficiente o espaço de armazenamento virtual e oferecer o máximo de desempenho de processamento com o menor impacto ou comprometimento da capacidade de processamento dos recursos tecnológicos da CONTRATANTE.
- 4.28. Os serviços devem estar aderentes às seguintes diretrizes culturais:
- 4.28.1. Todos os documentos e relatórios deverão ser produzidos em língua portuguesa, salvo quando autorizado pela CONTRATANTE.

#### Requisitos da Arquitetura Tecnológica

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

4.30. 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.

4.31. A arquitetura da Solução de TIC objeto do presente Termo de Referência deverá observar ao menos os seguintes princípios de excelência em operação de data center:

- 4.31.1. Permitir mudanças constantes, pequenas e frequentes.
- 4.31.2. O design das cargas de trabalho deve permitir que os componentes sejam atualizados com frequência.
- 4.31.3. Permitir a antecipação de falhas: Ser capaz de permitir a simulação de cenários, realização de teste e validação de requisitos antes de entrada em produção.

4.32. As arquiteturas criadas pela CONTRATADA em ambiente de data center devem:

- 4.32.1. Ser precedidas de planejamento,
- 4.32.2. Possuir cotas que limitem o consumo de determinado recurso de acordo com as necessidades da CONTRATANTE.
- 4.32.3. Permitir o gerenciamento de capacidade das cargas de trabalho com antecedência com vistas a evitar a limitação inesperada do consumo de recursos.
- 4.32.4. Prever mecanismos de controle de custos por meio de alertas relacionados a situações em que os gastos atinjam determinados limites.
- 4.32.5. Ser projetadas observando padrões mínimos de segurança, incluindo: controle de acesso, uso de mecanismos de log e de monitoramento, gestão de credenciais, segmentação de rede, entre outros recomendados pelo provedor..

#### Requisitos de Projeto e de Implementação

4.33. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.34. Os serviços de hospedagem deverão ser executados observando um projeto definido pela CONTRATADA e aprovado pela CONTRATANTE contendo no mínimo:

- 4.34.1. arquitetura da solução prevista em data center.
- 4.34.2. identificação das cargas de trabalho e recursos computacionais previstos.
- 4.34.3. considerações sobre segurança da informação.
- 4.34.4. estimativa de custos para os próximos três meses, no mínimo.

#### Requisitos de Implantação

4.35. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

- 4.35.1. A CONTRATADA deverá adotar mecanismos de automação e de implantação contínua.
- 4.35.2. Deverão ser adotadas práticas ágeis pela CONTRATADA na operação, implantação e automação de processos e cargas de trabalho no ambiente de data center.

#### Requisitos de Garantia e Manutenção

4.36. A CONTRATADA deverá reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos nos recursos e serviços de computação e de banco de dados, bem como a qualquer recurso do ambiente utilizado pela CONTRATANTE.

#### Requisitos de Experiência Profissional

4.37. Os serviços objeto da contratação deverão ser prestados por técnicos devidamente capacitados, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

#### Requisitos de Metodologia de Trabalho

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

#### Vistoria

- 4.42. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

#### Sustentabilidade

- 4.43. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

- 4.43.1. implementação de códigos que otimizem o consumo de recursos computacionais;
- 4.43.2. aumento da eficiência energética;
- 4.43.3. redução do consumo de papel, recursos de impressão e outros insumos não renováveis.

#### Subcontratação

- 4.44. É admitida a subcontratação parcial do objeto, nas seguintes condições:
- 4.44.1. É vedada a subcontratação completa ou da parcela principal do objeto da contratação, a qual consiste em serviço de hospedagem de aplicações e recursos de TIC;
- 4.44.2. A subcontratação fica limitada ao serviço de link de acesso do data center da CONTRATADA à internet, incluindo o serviço de proteção Anti-DDOS;
- 4.44.3. Quaisquer outras subcontratações estarão sujeitas à previa e expressa autorização da CONTRATANTE.

#### Garantia da Contratação

- 4.45. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.
- 4.46. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
- 4.47. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.
- 4.48. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

#### Informações relevantes para o dimensionamento e apresentação da proposta

- 4.49. A demanda do órgão tem como base as seguintes características:
- 4.49.1. O objeto desta licitação, considera a oferta de infraestrutura baseada em data center tradicional necessária aos serviços de hospedagem, armazenamento, processamento e comunicação de dados, com os sistemas e aplicativos da CONTRATANTE, fornecidos, também, os serviços de monitoramento, suporte técnico e backup/restore, garantindo a segurança física, lógica e a alta disponibilidade para atender o pleno funcionamento de todas as naturezas dos serviços a serem prestados; além dos serviços de comunicação de dados.

4.49.2. A CONTRATADA deverá realizar a atualização constante de hardware e software (com todo licenciamento incluso), devendo sempre primar pelas normas internacionais de Segurança da Informação e observar as práticas de gerenciamento de serviços de tecnologia definidas pela biblioteca de serviços ITIL (Information Technology Infrastructure Library).

4.49.3. A proposta deverá ser compatível com os preços praticados no mercado, sob pena de desclassificação.

4.49.4. Após a migração, haverá pagamentos mensais regulares, condicionados às metas de NÍVEIS MÍNIMOS DE SERVIÇO, podendo haver glosa de pagamento.

4.49.5. A CONTRATADA deve obrigatoriamente considerar em sua proposta o período de 36 (trinta e seis) meses de contrato, porém em até os 90 (noventa) dias após o início do serviço de migração como setup inicial do ambiente e o restante como operação.

4.49.6. Durante o período de implantação do ambiente (montagem dos ambientes de produção, desenvolvimento e homologação, instalação de links), não será devido nenhum pagamento mensal à CONTRATADA, somente será realizado o pagamento pelo serviço de migração quando de sua efetiva conclusão. Após o aceite definitivo da implantação haverá pagamentos mensais regulares.

4.49.7. O custo estimado da contratação encontra-se discriminado no item 1 deste Termo, bem como na planilha de custos em anexo a este documento.

4.49.8. No preenchimento da planilha de custos, deve ser utilizado o modelo em formato xlsx respeitando-se a formatação e fórmulas estabelecidas. Os preços individuais deverão ter exatamente 2 (duas) casas decimais.

4.49.9. A proposta de preços deverá conter os endereços dos data centers de propriedade da CONTRATADA onde ficarão hospedados os recursos de TIC, aplicações e dados da CONTRATANTE bem como a declaração das certificações que deverão ser apresentadas após o início de vigência do Contrato.

## 5. PAPÉIS E RESPONSABILIDADES

### 5.1. São obrigações da CONTRATANTE:

- 5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 5.1.2. 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;
- 5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;
- 5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;
- 5.1.8. 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:

- 5.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

- 5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 5.2.3. 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;
- 5.2.4. 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;
- 5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- 5.2.8. 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 CONTRATANTE;
- 5.2.9. fazer a transição contratual, conforme especificado neste documento.

## 6. MODELO DE EXECUÇÃO DO CONTRATO

### Condições de execução

#### 6.1. A execução do objeto seguirá a seguinte dinâmica:

- 6.1.1. Início da execução do objeto: na data de início da vigência do Contrato;
- 6.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:
  - 6.1.2.1. Da formalização da demanda:
    - 6.1.2.1.1. A formalização para início da prestação dos serviços deve ser realizada por meio de Ordem de Serviço (OS).
    - 6.1.2.1.2. A Ordem de Serviço deve ser elaborada conforme Anexo IX e encaminhada pelo Gestor do Contrato contendo no mínimo:
      - 6.1.2.1.3. a definição e a especificação dos serviços a serem realizados;
      - 6.1.2.1.4. o volume estimado de serviços a serem realizado;
      - 6.1.2.1.5. os prazos para realização dos serviços;
      - 6.1.2.1.6. o objetivo a ser alcançado, observando as metas de produtividade estabelecidas;
      - 6.1.2.1.7. a descrição do que deve ser executado;
      - 6.1.2.1.8. os produtos/resultados a serem entregues;
      - 6.1.2.1.9. os requisitos não funcionais;
      - 6.1.2.1.10. a identificação dos responsáveis da CONTRATANTE pelo acompanhamento dos serviços.
      - 6.1.2.1.11. a justificativa de necessidade da OS, seja um elemento pontual (e.g. alocação de uma máquina virtual) ou uma infraestrutura para um projeto;
      - 6.1.2.1.12. a justificativa dos parâmetros utilizados na OS (tipos de recursos, modalidades de fornecimento, duração da alocação dos recursos, capacidade dos recursos);



6.1.2.1.13. a análise de custo-benefício da OS com o enfoque na justificativa da economicidade e efetividade da escolha.

6.1.2.1.14. Com vistas a subsidiar a construção da ordem de serviço, a CONTRATANTE poderá solicitar a qualquer momento a elaboração de plano de arquitetura que deverá ser realizado conforme item Planejamento dos Serviços.

6.1.2.1.15. A elaboração de plano de arquitetura deve ser realizada sem ônus à CONTRATANTE.

6.1.3. Cronograma de realização dos serviços:

6.1.4. Os serviços serão executados em conformidade com as especificações da Ordem de Serviço (OS), bem como com os requisitos técnicos e temporais estabelecidos neste documento.

6.2. O serviço será prestado sob demanda, devendo a CONTRATADA atender às requisições e solicitações nos prazos previstos no NMS - Nível Mínimo de Serviços, sob pena de aplicação de glosas e retenções de pagamento, sem prejuízo da aplicação de penalidades cabíveis. Serão devidos à CONTRATADA somente os valores constantes da Planilha de Custos e da Proposta de Preços.

6.3. A Planilha de Custos, contém a estimativa inicial de recursos a serem fornecidos pela CONTRATADA, bem como os quantitativos máximos. Quanto ao provisionamento inicial, o Anexo VI informa com detalhes o ambiente inicial a ser provisionado durante o processo de migração.

#### Planejamento dos Serviços

6.4. Para os serviços que necessitem da realização de um planejamento, a CONTRATADA deverá agendar reunião com a CONTRATANTE em até 1 dia útil após a abertura do chamado ou recebimento da ordem de serviço, para tratar da demanda solicitada.

6.5. Após explicada a demanda solicitada pela CONTRATANTE, a CONTRATADA terá até 10 (dez) dias úteis para apresentar o plano de arquitetura de solução para implementação dos serviços demandados pela CONTRATANTE.

6.6. O prazo para apresentação do plano de arquitetura poderá ser ampliado à critério da CONTRATANTE.

6.7. O plano de arquitetura deverá conter, no mínimo, as seguintes informações:

6.7.1. Descrição detalhada do serviço a ser demandado;

6.7.2. Arquitetura proposta pela CONTRATADA para implementação do serviço demandado;

6.7.3. Orçamento detalhado dos recursos que serão usados pela CONTRATADA para implementação do serviço demandado com o preço efetivamente cobrado;

6.7.4. Prazo para entrega dos serviços em perfeita operação;

6.7.5. Descrição detalhada de restrições, dependências e quaisquer informações relevantes acerca do plano proposto.

6.8. Após entrega do plano de arquitetura, a CONTRATANTE realizará a análise de modo a verificar a aderência técnica e de negócio.

6.9. Havendo divergência, A CONTRATANTE solicitará à CONTRATADA que promova as adequações e/ou correções no plano de arquitetura, sem revisão do prazo e sem reinício de contagem de prazo, salvo quando a CONTRATANTE identificar algum fato impeditivo.

6.10. Após o aceite do plano de arquitetura, a CONTRATANTE analisará o plano e decidirá se os serviços a serem demandados serão implementados.

#### Local e horário da prestação dos serviços

6.11. Os serviços serão prestados remotamente pela CONTRATADA nos horários de funcionamento regular da CONTRATANTE, salvo quando houver solicitação expressa conforme discriminado neste documento.

#### Materiais a serem disponibilizados

6.12. Para a perfeita execução dos serviços, a CONTRATADA deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, promovendo sua substituição quando necessário.

6.13. A disponibilização dos Materiais descritos nesta seção deverá ser realizada sem ônus adicional à CONTRATANTE.

*Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)*

6.14. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo 36 (trinta e seis) meses, contado da data de início de vigência do Contrato.

Formas de transferência de conhecimento

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

6.15.1. A CONTRATADA deverá realizar o repasse de conhecimento à equipe de técnicos da CONTRATANTE, durante a vigência do contrato por meio de reuniões ou envio de documentos e informações, sempre que solicitado pela CONTRATANTE, com vistas a mitigar riscos de descontinuidade de serviços e de dependência técnica.

6.15.2. A transferência de conhecimento, no uso das soluções desenvolvidas pela CONTRATADA, deverá ser viabilizada, sem ônus adicionais para a CONTRATANTE, em eventos específicos de transferência de conhecimento, preferencialmente de forma remota, ou presencial quando houver informações consideradas pela CONTRATANTE com potencial de comprometimento da segurança da informação.

6.15.3. O cronograma e horários dos eventos deverão ser previamente aprovados pela CONTRATANTE.

6.15.4. A transferência de conhecimento, direcionada aos técnicos indicados pela CONTRATANTE, deverá ser focada na solução adotada, de forma que haja transferência do conhecimento da tecnologia utilizada nas diferentes cargas de trabalho do órgão em produção.

6.15.5. A CONTRATANTE poderá solicitar à CONTRATADA a formatação e realização de workshop para transferência do conhecimento técnico e operacional da solução à equipe técnica da CONTRATANTE.

6.15.6. As atividades de transferência de conhecimento ocorrerão sem ônus para a CONTRATANTE.

6.15.7. O não atendimento às demandas da CONTRATANTE por transferência de conhecimento configura inexecução parcial do contrato e expõe a CONTRATADA às penalidades previstas neste instrumento.

6.15.7.1. Entre os assuntos, devem-se constar a interação e a operação dos recursos tecnológicos em data center.

6.15.7.2. O plano do workshop deve ser elaborado pela CONTRATADA com o apoio da CONTRATANTE e ser entregue pelo menos cinco dias úteis anteriores ao início do workshop. O workshop deverá estar dimensionado para até 20 técnicos/analistas.

6.15.7.3. O workshop deverá contar com material didático desenvolvido pela CONTRATADA, ser realizado em local definido pela CONTRATANTE, dividido em turmas de acordo com a capacidade física do local e do tipo de transferência e ocorrerá pelo menos trinta dias corridos antes do encerramento do contrato.

6.16. A transferência de conhecimento poderá ser substituída, a critério da CONTRATANTE, por repasse documental definido entre as partes.

Procedimentos de transição e finalização do contrato

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

6.17.1. A CONTRATADA é responsável executar, sem qualquer ônus adicional para a CONTRATANTE ou para a futura CONTRATADA, todas as atividades necessárias para a correta e tempestiva migração do ambiente para a empresa sucessora na prestação dos serviços, na forma estabelecida pela CONTRATANTE, inclusive fornecendo trabalho das equipes técnicas no planejamento e execução da migração e do encerramento do contrato e disponibilizando softwares, recursos para replicação de ambiente e instalação de link de interconexão de data centers (Golden Jumper);

6.17.2. A CONTRATADA deverá disponibilizar as imagens de máquinas virtuais, discos virtuais e todos os demais dados de propriedade da CONTRATANTE, inclusive aqueles armazenados como backup, através de meios de transporte/transmissão tais quais os mencionados no item referente à Migração de Ambiente;

6.17.3. A CONTRATADA fornecerá à futura CONTRATADA acesso à camada de virtualização dos seus ambientes, para que esta instale os respectivos appliances de migração e replicação automatizadas;

6.17.4. A CONTRATADA deverá, no prazo máximo de 30(trinta) dias contados da solicitação da CONTRATANTE, emitir um termo informando que os dados foram destruídos, de acordo com o padrão NIST 800-88.

Quantidade mínima de serviços para comparação e controle

6.18. Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo.

Mecanismos formais de comunicação

6.19. São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

- 6.19.1. Ordem de Serviço;
- 6.19.2. Ata de Reunião;
- 6.19.3. Ofício;
- 6.19.4. Sistema de abertura de chamados;
- 6.19.5. E-mails e Cartas.

Formas de Pagamento

6.20. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.21. 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.

6.22. 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 V e VI deste documento.

## 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 representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. A Contratada 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. A Contratada deverá manter preposto da empresa disponível para contato durante horário comercial.

7.7. Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada 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.

7.9.1. A pauta desta reunião observará, pelo menos:

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

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

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

7.9.1.4. 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;

#### Fiscalização

7.10. 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) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

#### Fiscalização Técnica

7.11. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, 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. (Decreto nº 11.246, de 2022, art. 22, VI);

7.11.1. 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. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.11.2. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.11.3. 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. (Decreto nº 11.246, de 2022, art. 22, IV).

7.11.4. 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. (Decreto nº 11.246, de 2022, art. 22, V).

7.11.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

#### Fiscalização Administrativa

7.12. 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 do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.12.1. 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; (Decreto nº 11.246, de 2022, art. 23, IV).

#### Gestor do Contrato

7.13. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará 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. (Decreto nº 11.246, de 2022, art. 21, IV).

7.14. O gestor do contrato acompanhará 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. (Decreto nº 11.246, de 2022, art. 21, II).

7.15. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.16. O gestor do contrato emitirá 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. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.17. O gestor do contrato tomará 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. (Decreto nº 11.246, de 2022, art. 21, X).

7.18. O gestor do contrato deverá 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. (Decreto nº 11.246, de 2022, art. 21, VI).

7.19. O gestor do contrato deverá 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.

## 8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A contratada será remunerada pelo serviço efetivamente prestado como o valor de cada serviço contratado constante da planilha de custos em anexo ao presente Termo de Referência, observando o adimplemento dos níveis mínimos de serviços definidos.

8.2. O faturamento mensal será calculado de acordo com a seguinte fórmula:

$$Fm = \text{soma}(P \times Q) - \text{soma}(\text{ajuste NMS})$$

onde:

Fm: faturamento mensal a ser pago à contratada;

P: preço de cada serviço constante da planilha de custos;

Q: quantidade de serviços efetivamente consumidos;

ajuste NMS: valor total de desconto, aplicado em virtude de não atendimento dos níveis mínimos de serviço pela Contratada.

8.3. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme o disposto neste item.

INDICADOR DE DISPONIBILIDADE DO ACESSO AO DATA CENTER VIA LINK DE SAÍDA (IDADC)	
Tópico	Descrição

Finalidade	O IDADC visa aferir o percentual do tempo em que os serviços de hospedagem estiveram acessíveis no mês.	
Meta a cumprir	IDADC >= 99,741%	O acesso ao data center via link de internet deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o período de vigência do contrato.
Instrumento de medição	Através da plataforma de monitoramento de link de dados e por controle próprio da CONTRATANTE, na constatação de indisponibilidade de acesso.	
Forma de acompanhamento	Durante a execução dos serviços, a disponibilidade será monitorada e permanentemente.	
Periodicidade	Será aferida mensalmente.	
Mecanismo de Cálculo (métrica)	O IDADC será calculado através do sistema de monitoramento da CONTRATADA bem como por ferramentas de monitoração próprios da CONTRATANTE, calculado em percentual do tempo de disponibilidade do link de saída do data center para a internet.	
Observações	A glosa será aplicada sobre o custo mensal do serviço de fornecimento de link de acesso à internet estabelecido na Planilha de Custos.	
Início de Vigência	A partir da emissão do início da prestação dos serviços e após concluído o processo de migração de data center.	
Faixas de ajuste no pagamento	<p>Base de cálculo:</p> <p>Corresponde ao custo mensal do serviço de fornecimento de link de acesso à internet estabelecido na Planilha de Custos.</p> <p>Para valores do indicador IDADC:</p> <p>Igual ou Superior a 99,741% – Pagamento integral do valor mensal do serviço;</p> <p>De 99,00% a 99,741% - Glosa de 10% sobre o valor da base de cálculo;</p>	

	De 98,00% a 99,00% - Glosa de 20% sobre o valor da base de cálculo.
--	---

<b>INDICADOR DE ATENDIMENTO AO SUPORTE TÉCNICO A INCIDENTES E REQUISIÇÕES DE SERVIÇOS (IASTIS)</b>		
Tópico	Descrição	
Finalidade	O IASTIS visa mensurar a execução dos serviços de atendimento a incidentes e gerenciamento de recursos nos prazos máximos estabelecidos.	
Meta a cumprir	IASTIS >= 95 %	Executar as operações e atividades dentro dos prazos para a execução previstos no item 2 do presente Termo de Referência e na ordem de serviço.
Instrumento de medição	Através dos sistemas de ITSM/ITIL da CONTRATADA e validado pelo respectivo sistema da CONTRATANTE.	
Forma de acompanhamento	Após a execução dos serviços, os fiscais analisarão individualmente cada execução de serviço verificando a conclusão no prazo definido neste Termo de Referência.	
Periodicidade	Será aferido mensalmente.	
Mecanismo de Cálculo (métrica)	<p><math>IASTIS = (TCSA / TC) \times 100</math></p> <p>Onde:</p> <p>IASTIS = Percentual de serviços entregues tempestivamente.</p> <p>TC = Total de chamados ocorridos no mês (incidentes ou requisição de serviços)</p> <p>TCSA = Total de chamados sem atraso.</p>	
Observações	A glosa será aplicada sobre 20% do total do item 1 da contratação, ou seja, serviço de hospedagem em data center.	
Início de Vigência	A partir da emissão do início da prestação dos serviços e após concluído o processo de migração de data center.	
	Base de cálculo:	

Faixas de ajuste no pagamento	<p>Corresponde 20% do total mensal do item 1 da contratação, ou seja, serviço de hospedagem em data center.</p> <p>Para valores do indicador IASTIS:</p> <p>Igual ou Superior a 95% – Pagamento integral do faturamento mensal;</p> <p>De 90,00% a 95,00% - Glosa de 10% sobre o valor da base de cálculo;</p> <p>De 80,00% a 90,00% - Glosa de 20% sobre o valor da base de cálculo.</p>
-------------------------------	---

INDICADOR DE ENTREGA DE RELATÓRIOS TÉCNICOS PARA FATURAMENTO (IERTF)		
Tópico	Descrição	
Finalidade	O IERTF visa mensurar a entrega tempestiva de relatórios técnicos essenciais à correta medição do faturamento mensal	
Meta a cumprir	IERTF $\leq$ 0	Executar a entrega dos relatórios e documentos técnicos para fins de medição de faturamento até o quinto dia útil do mês seguinte à entrega do serviço conforme estabelecido neste documento.
Instrumento de medição	Relatórios e documentos emitidos pela CONTRATADA.	
Forma de acompanhamento	Após o início de vigência do contrato, os fiscais analisarão a entrega de documentos e relatórios necessários à apuração mensal do faturamento, verificando a conclusão no prazo definido neste Termo de Referência.	
Periodicidade	Será aferido mensalmente após a conclusão de cada etapa do serviço.	
Mecanismo de Cálculo (métrica)	<p>IERTF = PR - PMP</p> <p>Onde:</p>	



	<p>IERTF = Dias úteis de entrega do serviço dentro do prazo previsto.</p> <p>PMP = Prazo máximo em dias úteis previsto para entrega dos relatórios e documentos (5 dias úteis).</p> <p>PR= Prazo realizado em dias úteis.</p>
Observações	<p>Serão utilizados dias úteis na medição.</p> <p>O período cuja pendência dependa da CONTRATANTE será descontado da forma de cálculo.</p> <p>A glosa será aplicada sobre 20% do total do item 1 da contratação, ou seja, serviço de hospedagem em data center.</p>
Início de Vigência	A partir do início de vigência do Contrato.
Faixas de ajuste no pagamento	<p>Base de cálculo:</p> <p>Corresponde a 20% do total mensal do item 1 da contratação, ou seja, serviço de hospedagem em data center.</p> <p>Para valores do indicador IERTF:</p> <p>Igual ou inferior a 0 – Pagamento integral do faturamento mensal;</p> <p>De 1 a 5 – Glosa de 3% sobre o valor da base de cálculo;</p> <p>De 6 a 10 – Glosa de 5% sobre o valor da base de cálculo;</p> <p>De 11 a 15 – Glosa de 7% sobre o valor da base de cálculo;</p> <p>De 16 a 30 - Glosa de 10% sobre o valor da base de cálculo e aplicada advertência.</p> <p>Acima de 30 – Será declarado não execução do serviço, sem prejuízo da aplicação de glosa anterior.</p>

INDICADOR DE TEMPESTIVIDADE NA MIGRAÇÃO (ITM)		
Tópico	Descrição	
Finalidade	Mensurar a execução dos serviços de migração nos prazos máximos estabelecidos	
Meta a cumprir	ITM $\leq$ 0	Executar a migração do ambiente dentro dos prazos para a execução previstos no item 2 do Termo de Referência.
Instrumento de medição	Ordens de Serviço emitidas, bem como relatórios e documentos emitidos pela fiscalização do contrato.	
Forma de acompanhamento	Após o início de vigência do contrato, os fiscais analisarão cada etapa da migração de ambiente, verificando a conclusão no prazo definido neste Termo de Referência.	
Periodicidade	Será aferido uma única vez durante o processo global de migração de ambiente.	
Mecanismo de Cálculo (métrica)	<p>ITM = PR - PMP</p> <p>Onde:</p> <p>ITM = Dias de entrega do serviço dentro do prazo previsto.</p> <p>PMP = Prazo Máximo previsto para migração.</p> <p>PR= Prazo realizado.</p>	
Observações	<p>Serão utilizados dias corridos na medição.</p> <p>O período cuja pendência dependa da CONTRATANTE será descontado da forma de cálculo.</p> <p>A base de cálculo será o custo total do serviço de migração estabelecido na Planilha de Custos.</p>	
Início de Vigência	A partir do início de vigência do Contrato.	
Faixas de ajuste no pagamento	<p>A base de cálculo será o custo total do serviço de migração estabelecido na Planilha de Custos.</p> <p>Para valores do indicador ITM:</p> <p>Igual ou inferior a 0 – Pagamento integral da base de cálculo;</p>	

	De 1 a 5 – Glosa de 3% sobre o valor da base de cálculo;
	De 6 a 10 – Glosa de 5% sobre o valor da base de cálculo;
	De 11 a 15 – Glosa de 7% sobre o valor da base de cálculo;
	De 16 a 30 - Glosa de 10% sobre o valor da base de cálculo e aplicada advertência.
	Acima de 30 – Será declarado não execução do serviço de migração, sem prejuízo da aplicação de glosa anterior.

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

- 8.4.1. não produzir os resultados acordados;
- 8.4.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou
- 8.4.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

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

#### Do recebimento

8.6. Os serviços serão recebidos provisoriamente, no prazo de 5 (cinco) dias úteis, 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 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

- 8.6.1. 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.

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. (Art. 22, X, Decreto nº 11.246, de 2022).

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. (Art. 23, X, Decreto nº 11.246, de 2022)

8.9. 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.

- 8.9.1. 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;

8.10. 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.

8.11. 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. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

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

8.13. 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.

8.14. 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.

8.15. Os serviços serão recebidos definitivamente no prazo de 5 (cinco) dias úteis, 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:

8.15.1. 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);

8.15.2. 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;

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

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

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

8.16. 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 concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

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

8.18. 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

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

8.19.1. A CONTRATANTE poderá realizar auditorias, inclusive com apoio de terceira parte, para comprovar que a CONTRATADA mantém os requisitos de testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades e avaliação de segurança dos serviços);

8.19.2. A critério da CONTRATANTE, testes poderão ser realizados a fim de comprovar as funcionalidades e a especificação proposta neste Termo de Referência;

8.19.3. Na ausência de especificações idênticas às mínimas exigidas, serão aceitas especificações superiores.

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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

--	--	--

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência.
2	Não cumprir as condições mínimas exigidas no item Requisitos de Emissão da OS	Multa de 1% do valor total do contrato, sem prejuízo de declaração de inexecução total do objeto.
3	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A CONTRATADA ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores, pelo prazo de até 3 (três) anos, sem prejuízo das demais cominações legais.
4	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A CONTRATADA será declarada inidônea para licitar e contratar com a Administração.
5	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	A CONTRATADA ficará impedida para licitar e contratar com a Administração por 6 (seis) meses, sem prejuízo da Rescisão Contratual.
6	Não executar os serviços previstos no objeto da contratação.	Multa de até 3% sobre o valor total do Contrato.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao Gestor do Contrato.	Multa de até 3% sobre o valor total do Contrato.

8	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 estabelecido neste Termo de Referência	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplicar-se-á multa de 1% do valor referente a parcela mensal apurada do Contrato.
9	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da CONTRATANTE.	A CONTRATADA será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato.
10	Não atender ao indicador de nível mínimo de serviço indicador de disponibilidade do acesso ao data center via link de saída (IDADC).	Para valor abaixo de 98%, aplicar-se-á multa de 5% do valor total do contrato.
11	Não atender ao indicador de nível mínimo de serviço indicador de atendimento ao suporte técnico incidentes e requisições de serviços (IASTIS)	Para valor abaixo de 80,00%, aplicar-se-á multa de 4% do valor total do contrato.
12	Não atender ao indicador de nível mínimo de serviço indicador de entrega de relatórios técnicos para faturamento (IERTF)	Para valor acima de 30, aplicar-se-á multa de 3% do valor total do contrato e será declarado a não execução do serviço de gerenciamento e sustentação mensal, sem prejuízo da aplicação de glosa e sanção anterior.
13	Não atender ao indicador de nível mínimo de serviço indicador de tempestividade na migração (ITM).	Para valor acima de 30, aplicar-se-á multa de 3% do valor total do contrato e será declarado a não execução do serviço de migração, sem prejuízo da aplicação de glosa e sanção anterior.

14	Deixar de disponibilizar o(s) profissional(is) que irão desempenhar os serviços no prazo máximo de 5 (cinco) dias úteis após a emissão da Ordem de Serviço (OS), com os requisitos mínimos de experiência e formação profissional.	Não havendo o cumprimento desta obrigação por igual período, será aplicada multa de 0,1% do valor total do item associado ao serviço objeto da OS por dia corrido de atraso, limitado a 5%.
15	<p>Vazamento ou permissão de acesso por terceiros às informações sem prévia autorização formal do órgão proprietário e da CONTRATANTE ou autorização legal pela Justiça brasileira;</p> <p>Não informação à CONTRATANTE de solicitação de acesso aos dados e informações por parte de terceiros ou governos estrangeiros, mesmo se respaldado em autorização judicial não respaldada pela Justiça brasileira;</p> <p>Falhas de criptografia ou armazenamento de chaves que possibilitem o acesso indevido às informações sob a guarda da CONTRATADA;</p> <p>Falha no serviço de backup que impeça a restauração de dados copiados, sem prejuízo da cobrança pelo serviço de recuperação das informações eventualmente perdidas e outras ações inclusive judiciais cabíveis;</p>	multa de 5% (cinco por cento) sobre o valor total do contrato e rescisão unilateral por descumprimento contratual, sem prejuízo de outras sanções cabíveis
16	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	<p>Advertência.</p> <p>Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplicar-se-á multa de 5% do valor referente a parcela mensal apurada do Contrato.</p>

8.21. 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 a CONTRATADA:

8.21.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.21.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada.

#### Liquidação

8.22. 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, §2º da Instrução Normativa SEGES/ME nº 77/2022.

8.23. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso 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.

8.24. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

8.24.1. o prazo de validade;

8.24.2. a data da emissão;

8.24.3. os dados do contrato e do órgão contratante;

8.24.4. o período respectivo de execução do contrato;

8.24.5. o valor a pagar; e

8.24.6. eventual destaque do valor de retenções tributárias cabíveis.

8.25. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, 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;

8.26. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado 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, de 2021.

8.27. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018)

8.28. 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.

8.29. 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.

8.30. 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.

8.31. 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

8.32. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.



8.33. No caso de atraso pelo CONTRATANTE, os valores devidos a CONTRATADA 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

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

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

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

8.37. 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.

8.38. 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.

#### Cessão de crédito

8.39. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

8.39.1. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

8.40. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

8.41. 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.

8.42. 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 (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020).

8.43. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

#### Reajuste

8.44. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI com periodicidade conforme definido no § 3º do art. 92 da Lei nº 14.133/21.

### 9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

#### Forma de seleção e critério de julgamento da proposta

9.1. 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 GLOBAL DO LOTE.

9.2. O Modo de Disputa será ABERTO E FECHADO, tendo em vista o grau de padronização e homogeneização do objeto a ser contratado. Assim as licitantes terão acesso ao valor estimado da contratação porém durante a fase de lances ocorrerá com omissão dos valores ofertados pelas empresas durante a disputa, sendo estes somente revelados após o final da etapa competitiva.

9.3. De forma a fornecer os insumos para que a análise de exequibilidade da proposta possa ser feita, a LICITANTE deverá apresentar a Planilha de Custos junto com a Proposta de Preços.

#### Regime de execução

9.4. O regime da execução do contrato é de EMPREITADA POR PREÇO GLOBAL, uma vez que consegue-se definir de antemão a qualidade e a quantidade serviços a serem prestados com boa margem de segurança

#### Da Aplicação da Margem de Preferência

9.5. Não será aplicada, na presente contratação, margem de preferência prevista no art. 26 da Lei nº 14.133, de 2021, uma vez que a sua utilização carece de regulamentação em normativo ainda não publicado.

#### Exigências de habilitação

9.6. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

#### Habilitação jurídica

9.7. 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;

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

9.9. 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>;

9.10. 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;

9.11. 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.

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

9.13. 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

9.14. 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.

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

#### Habilitação fiscal, social e trabalhista

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

9.17. 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.

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

9.19. 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;

- 9.20. Prova de inscrição no cadastro de contribuintes Estadual ou Municipal/Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 9.21. Prova de regularidade com a Fazenda Estadual ou Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 9.22. Caso o fornecedor seja considerado isento dos tributos Estadual ou Municipal/Distrital 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.
- 9.23. 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

- 9.24. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;
- 9.25. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);
- 9.26. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:
- 9.26.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);
- 9.26.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e
- 9.26.3. 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.
- 9.27. 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.
- 9.28. Caso a empresa licitante 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 capital mínimo ou patrimônio líquido mínimo de 5% do valor total estimado da contratação.
- 9.29. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).
- 9.30. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

#### Qualificação Técnica

- 9.31. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação;
- 9.31.1. A declaração acima poderá ser substituída por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação
- 9.32. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.
- 9.33. Entende-se por serviço equivalente ao objeto deste Termo de Referência atestado(s) que comprove(m) a prestação de serviços continuados (mínimo de 30 meses), para serviços de hospedagem em data center, englobando serviços de fornecimento e suporte técnico para servidores virtuais, banco de dados, acesso à internet, serviços de backup e segurança da informação.

9.33.1. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

9.34. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.35. 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 da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9.36. A proponente deverá apresentar declaração com a indicação de que o ambiente de data center de sua propriedade que irá hospedar os dados da CONTRATANTE estará em território brasileiro, e que terá certificação Tier III (Tier Standards) ou Tier 3 (EIA/TIA 942) conforme disposto no art. 67, inciso III da Lei nº 14.133/2021. O comprovante da respectiva certificação deverá ser apresentado em até 10 (dez) dias após a data de início de vigência do Contrato.

9.37. A proponente deverá apresentar declaração de que o ambiente de data center de sua propriedade que irá hospedar os dados da CONTRATANTE está em conformidade com Service and Organization Controls 2 (SOC-2) - padrões de segurança, por meio de auditoria anual SOC-2, conduzida por um auditor independente, conforme disposto no art. 67, inciso III da Lei nº 14.133/2021. O relatório de tipo II deverá ser apresentados em até 10 (dez) dias após a data de início de vigência do Contrato.

## 10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação encontra-se especificado no item 1 deste Termo de Referência e na Planilha de Custos em anexo a este documento.

## 11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

11.2. A contratação será atendida pela seguinte dotação:

- I) Gestão/Unidade: 17203/173039
- II) Fonte de Recursos: 1050000294
- III) Programa de Trabalho: 04122003220000001
- IV) Elemento de Despesa: 33904009
- V) Plano Interno: SUSEPSI2000

11.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

### Cronograma Físico Financeiro

Evento	Prazo estimado	Valor
Migração de ambiente	Até 90 (noventa) dias após a data constante da Ordem de Serviço correspondente. Pagamento em parcela única	Conforme o item correspondente da planilha de custos - Migração de Ambiente
Serviço de hospedagem em data center	Pagamento mensal após o fim do processo de migração de ambiente até o final do Contrato	Conforme estabelecido na planilha de custos e apurado pela fiscalização do contrato

## ANEXOS

ANEXO I - Planilha de Custos

ANEXO II – Proposta de Preços

ANEXO III - Planilha de Volumetria Atual

ANEXO IV - Requisitos de Migração de Data Center

ANEXO V - Termo de Ciência

ANEXO VI - Carta de Apresentação de Preposto

ANEXO VII - Termo de Compromisso de Manutenção do Sigilo

ANEXO VIII - POSIC/SUSEP

ANEXO IX – Modelo de Ordem de Serviço

ANEXO X - Termo de Recebimento Provisório de Serviços de TIC

ANEXO XI - Termo de Recebimento Definitivo

## 2. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

**LUIZ EDUARDO ADEMI TEIXEIRA**

Integrante Técnico



*Assinou eletronicamente em 02/10/2024 às 12:15:48.*