Termo de Referência 63/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
63/2024	560010-COORDENAçãO GERAL DE RECURSOS LOGISTICOS MCID	ALINE BARROS DE SOUSA	07/01/2025 18:06 (v 6.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC	13/2024	80000.000362/2024-15

1. Condições gerais da contratação

Contratação de empresa para o fornecimento de solução de segurança de rede composta por uma solução de Next Generation Firewall (NGFW), contemplando todos os softwares necessários, licenciamento, instalação, configuração, suporte, garantia, suporte técnico, repasse de conhecimento, Gerenciamento de LOGS e Automação, Gerenciamento Centralizado, conforme as especificações técnicas e operacionais descritas neste projeto, visando atender às necessidades do Ministério das Cidades, conforme condições e exigências estabelecidas neste instrumento.

LOTE	ITEM	DESCRIÇÃO	SUB-DESCRIÇÃO	CATMAT/CATSER	UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO	VALOR TOTAL POR ITEM
1	1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall(NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Hardware/Licenciamento	481646	Unidade	4	R $ 1.896.136,16	R $ 7.584.544,64
	2	Solução para Gerenciamento de LOGS e Automação		27014	Unidade	1	R $ 137.419,70	R $ 137.419,70
	3	Solução para Gerenciamento Centralizado de NGFW		27014	Unidade	1	R $ 88.123,00	R $ 88.123,00
	4	Instalação e Configuração		26972	Unidade	1	R $ 67.514,24	R $ 67.514,24
VALOR GLOBAL ESTIMADO								**R $ 7.877.601,58**

O item 1 contempla a implantação de uma solução de segurança perimetral de alta disponibilidade, baseada em cluster de firewalls de próxima geração (NGFW). A arquitetura proposta, composta por dois clusters com duas unidades cada, totalizando quatro equipamentos, garante a continuidade do serviço e a escalabilidade necessária para atender às demandas crescentes do Ministério das Cidades.

As quantidades apresentadas na tabela acima se baseiam na estrutura prevista para o Ministério das Cidades.

O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

Os serviços objeto desta contratação são caracterizados como comuns, uma vez que seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado.

O prazo de vigência da contratação é de 60 (sessenta) meses contados da assinatura do contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

O fornecimento de bens é enquadrado como continuado tendo em vista que fornecimento da soluação prevê suporte, garantia e licenciamento inclusos para 60 meses contínuos, sendo a vigência plurianual mais vantajosa considerando demonstrado em nosso Estudo Técnico Preliminar COINFRA-MCID (SEI nº 5530101), em que se observa dentro do período estimado a melhor relação de custo-benefício que se adequa e atende a todos os aspectos técnicos vislumbrados na demanda do Ministério nesta contratação de solução de Segurança da Informação de TIC.

O objeto da contratação não incide nas hipóteses vedadas pelos artigos 3º, 4º e 5º da IN SGD nº 94/2022.

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

2. Descrição da solução

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

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

A solução de TIC consiste em solução de segurança de rede composta por uma solução de Next Generation Firewall (NGFW), incluindo prevenção de ameaças avançadas, proteção DNS, anti-phishing, inspeção SSL e gerenciamento unificado. Essa solução deverá englobar todos os softwares necessários, licenciamento dos equipamentos e assinaturas de serviços de segurança, além da implantação, garantia de atualização contínua e suporte técnico. Durante o período de garantia, deverá haver um repasse de conhecimento conforme as especificações técnicas e operacionais descritas neste projeto, visando atender às necessidades do Ministério das Cidades.

Assim, a solução a ser contratada terá como composição:

ITEM	DESCRIÇÃO	SUB-DESCRIÇÃO	UNIDADE DE MEDIDA	QTD
1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall(NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Hardware /Licenciamento	Unidade	4
2	Solução para Gerenciamento de LOGS e Automação		Unidade	1
3	Solução para Gerenciamento Centralizado de NGFW		Unidade	1
4	Instalação e Configuração.		Unidade	1

A solução deverá observar integralmente os requisitos descritos abaixo:

CARACTERISTICAS GERAIS DA SOLUÇÃO

ITEM 1 - NEXT GENERATION FIREWALL(NGFW)

A solução proposta será um Firewall NGFW de última geração e não um sistema UTM;

A solução proposta deve ter pelo menos uma porta dedicada para console e pelo menos uma porta USB;

Deverá ser entregue dois equipamentos idênticos para cada cluster de NGFW solicitado;

A solução proposta deve ter pelo menos 8 interfaces Gigabit Ethernet, que podem ser portas de interface WAN ou LAN;

A solução deve possuir no mínimo 6 interfaces SPF+ 10Gb + 14 interfaces do tipo SFP 1Gb;

A solução deve possuir um par de portas dedicadas para HA, com velocidade de 10Gb em SFP+;

A solução deve possuir throughput de no mínimo 15 Gbps para Threat Protection, ou seja, com funcionalidades de IPS, Antivirus /Anti-Malware, Controle de Aplicação e Filtragem de URL habilitadas;

A solução deve possuir throughput de no mínimo 25 Gbps para NGFW, ou seja, com assinaturas de IPS e controle de aplicação habilitados;

A solução deve suportar 14 milhões de sessões simultâneas;

A solução deve suportar 600 mil novas sessões por segundo;

A solução deve possuir um Throughput mínimo de IPSec VPN a 20 Gbps;

A solução deve possuir um Throughput mínimo de de IPS de 28 Gbps;

A solução proposta deve ter um espaço de armazenamento mínimo de 900GB SSD e permitir expansão de disco para pelo menos 1.9TB SSD, apenas com a substituição de discos no mesmo equipamento;

Deverá possuir fonte de alimentação redundante capaz de manter a operação total do equipamento mesmo em caso de falha de uma das fontes.

A solução não deve ter chips específicos de aplicativos, como ASICs, que não permitem futuras expansões de firmware e recursos no mesmo hardware. A solução deve ser baseada em arquitetura de processamento paralelo e não deve utilizar chips ASIC proprietários.

Serviços de Rede e Roteamento

A solução proposta deve ser capaz de operar no modo Camada 3 (roteamento), bridge e Camada 2 (espelhamento de porta) simultaneamente (sem necessidade de virtualizar o equipamento);

A solução proposta deve suportar protocolos de roteamento dinâmico OSPF, BGP e RIPv2;

A solução proposta deve suportar o roteamento estático e baseado em políticas (PBR);

A solução proposta deve suportar roteamento baseado em aplicativos, a fim de rotear aplicativos como P2P, vídeo on-line, etc. Com números dinâmicos de porta para o link WAN selecionado;

A solução proposta deve suportar os serviços de rede proxy DHCP, NTP, DNS Server e DNS;

A solução proposta deve suportar o roteamento ou o modo de operação NAT;

A solução proposta deve ser configurada no modo TAP;

A solução proposta deve ser compatível com o modo de operação transparente (bridge);

A solução proposta deve suportar o modo de operação misto (NAT, roteamento e bridge);

A solução proposta deve suportar os seguintes modos de interface: sniffer, port aggregation, loopback, VLANS (802.1Q e Trunking);

A solução proposta deve suportar switching e roteamento (Camada 2 e Camada 3);

A solução proposta deve suportar o recurso de switch virtual. Cada switch virtual deve ter sua própria tabela de endereços MAC;

A solução deverá constar no último quadrante mágico do Gartner para Next Generation Firewall no quadrante de líderes ou visionários;

A solução proposta deve suportar o recurso de roteamento virtual. Cada roteador virtual deve ter sua própria tabela de roteamento;

A solução proposta deve suportar a espelhamento de tráfego;

A solução proposta deve suportar SNAT, DNAT e PAT;

A solução proposta deve suportar NAT dinâmico e NAT estático, NAT N:1, NAT 1:N e 1:1 NAT;

A solução deve suportar NAT444 (CGNAT);

A solução deve suportar detecção de encaminhamento bidirecional (BFD), interação BFD com rota estática, OSPF ou BGP;

A solução proposta deve suportar a expansão do grupo NAT para um endereço IPv4 público para suportar mais de 64K endereços IP privados;

A solução proposta deve suportar NAT46, NAT64, DNS64;

A solução proposta deve suportar Full Cone NAT;

A solução proposta deve suportar o recurso NetFlow, o dispositivo pode coletar tráfego de entrada do usuário e enviá-lo para o servidor com a ferramenta de análise de dados NetFlow, para detectar, monitorar e coletar tráfego;

Deve suportar visualização de informações de status de link de várias interfaces ao mesmo tempo para análise comparativa;

A solução deve suportar o balanceamento de carga de servidor;

A solução deve suportar proteção de sessão, persistência de sessão e monitoramento do status da sessão;

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

A solução deve suportar a verificação de saúde do servidor, o monitoramento da sessão e a proteção da sessão;

A solução deve suportar o balanceamento de carga de link bidirecional;

A solução deve suportar a proteção contra sobrecarga de link, o tráfego mudará para outras ligações quando a conexão atual estiver sobrecarregada; o sistema continuará monitorando a largura de banda dos links e bloqueando novas sessões para o link que está sobrecarregado de acordo com as configurações do limiar;

A solução deve suportar a inspeção estatal de link com ARP, PING e DNS;

A solução deve suportar o gerenciamento de dispositivos sobre IPv6, registro IPv6 e HA no IPV6;

A solução deve suportar túneis IPv6, DNS64/NAT64;

A solução deve suportar protocolos de roteamento IPv6 para roteamento estático, roteamento RIPng, OSPFv3 e BGP4+;

A solução deve suportar VPN IPSec para IPv6;

A solução deve ser compatível com HA, nos modos Ativo/Ativo e/ou Ativo/Passivo;

A solução deve suportar interfaces de heartbeat redundantes para HA;

Em HA a solução deve sincronizar: sessões de firewall, associações de VPN, configurações, tabela ARP, tabela MAC e informações de DHCP;

A solução deve suportar HA no modo peer, para evitar problemas de roteamento assimétrico na implementação do modo Active-Active.

Controle de Políticas de Firewall

A solução deve suportar o uso de objetos em políticas, dos tipos predefinidos e personalizados;

A solução proposta deve suportar a política de segurança baseada em aplicativos, usuários/grupos de usuários e localização geográfica;

A solução proposta deve suportar a ALG (Application Layer Gateway) para pelo menos os seguintes protocolos: MSRCP, RSH, RTSP, SIP, FTP, TFTP, HTTP, H245 e H323;

A solução proposta deve permitir a criação de uma única política para controle de aplicativos, controle baseado no usuário, prevenção de ameaças, antivírus, filtragem de arquivos, dentro de uma única política;

A solução deve suportar a verificação da redundância da política de segurança;

A solução deve ser compatível com a política programada (agendamento), onde seja possível configurar o horário para ação de uma política, permitindo por exemplo, criar uma política mais permissiva no horário de almoço;

A solução proposta deve suportar o limite de sessão com base no IP de origem, IP de destino, protocolo e limitar novas conexões;

A solução proposta deve suportar defesa contra-ataques de protocolos anormais;

Solução proposta deve suportar defesa contra-ataques de ARP;

A solução deve suportar a proteção contra-ataques do tipo DDoS;

A solução deve suportar a proteção contra-ataques do tipo SYN Flood e UDP Flood;

Deve suportar o uso de zonas de segurança e diferentes configurações para diferentes zonas de segurança;

A solução deve suportar funcionalidades de IPS, AV e URL Filtering para tráfego criptografado SSL.

Prevenção de Ameaças

A solução deve suportar assinaturas personalizadas e atualizações automáticas de assinaturas;

A solução deve suportar proteção contra injeção SQL e ataques XSS;

A solução deve suportar proteção contra-ataques de C&C;

A solução deve suportar detecção de anomalias de protocolo, detecção rate-based ou característica similar;

A solução deve suportar as seguintes ações de IPS: apenas monitoramento, bloqueio e reset (IP do invasor ou IP da vítima);

A solução deve suportar proteção DoS rate-based para IPv4 e IPv6 com configurações de limites contra ataques de TCP Syn Flood, port scan, ICMP sweep, e session flooding;

A solução proposta deve suportar Reputação IP e bloqueio de IPs de servidores botnet fazendo uso de um banco de dados global de reputação de IPs;

A solução proposta deve ser compatível para filtrar assinaturas de IPS, procurando por CVE ID;

A solução deve efetivamente descobrir bots de intranet e evitar novos ataques avançados de ameaças, comparando as informações obtidas com o banco de dados de endereços C&C;

A solução deve suportar atualizações regulares de endereço do servidor Botnet;

A solução deve suportar dois tipos de banco de dados de endereços C&C: o banco de dados de endereços IP e o banco de dados de endereços de domínio;

A solução deve permitir a criação de white list de C&C (IPs e domínio);

A solução deve suportar o Antivírus baseado em fluxo de rede para os protocolos HTTP, POP3, SMB, FTP, SMTP e IMAP;

A solução deve suportar a detecção de vírus para arquivos compactados como RAR, ZIP, GZIP e TAR, permitindo a detecção de arquivos compactados em várias camadas, com suporte a no mínimo 5 camadas de descompressão;

A solução deve suportar advertência de vírus e sites maliciosos, alertando o usuário de que o site é um site malicioso ou que um vírus foi detectado;

A solução deve suportar o upload de arquivos maliciosos para análise em nuvem, utilizando funcionalidade de cloud sandbox totalmente licenciada;

A solução deve suportar o upload de arquivos maliciosos para sandbox para protocolos os protocolos HTTP, POP3, SMB, FTP, SMTP e IMAP;

A função de sandbox deve suportar tipos de arquivos que incluem PE/EXE, RAR, ZIP, MS Office, PDF, APK e JAR;

A solução deve suportar o controle do tamanho do arquivo que será enviado para análise no sandbox.

Controle de Aplicação e URL

A solução deve suportar filtro da Web definido manualmente com base em URL, conteúdo da Web e cabeçalho MIME;

A solução deve suportar substituir o perfil de filtro de URL, para que o administrador possa atribuir temporariamente diferentes perfis ao usuário/grupo/IP;

A solução deve permitir que se personalize a página de aviso para quando uma URL for bloqueada;

A solução deve suportar a configuração de filtro de URL com base na zona de segurança;

Deve possuir suporte para filtrar o tráfego de IPs de baixa reputação, incluindo Botnet, Spam, nódulos comprometidos, força bruta, etc;

Deve suportar atualizar o banco de dados de reputação de IP;

Suporte para filtrar o endereço IP de bots e servidor de botnet;

A solução deve suportar mais de 3.000 aplicações, deve suportar filtro de aplicativos por nome, categoria, subcategoria, tecnologia e nível de risco;

A solução deve suportar a visualização da descrição, fatores de risco, dependências, portas típicas usadas e URLs para referências adicionais e informações para cada aplicativo;

A solução deve ser capaz de identificar e controlar aplicações em nuvem, deve fornecer monitoramento incluindo categoria de risco e recurso;

A solução deve suportar o controle de transferência de arquivos com base no nome, tipo e tamanho do arquivo;

A solução deve suportar o controle de transferência de arquivos nos seguintes protocolos: HTTP, HTTPS, FTP, SMTP, POP3;

A solução deve suportar a autenticação do usuário com LDAP, Radius e Active Directory;

A solução deve suportar a sincronização de grupos de usuários baseados em AD e LDAP;

A solução deve suportar 802.1X;

Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

A solução deve possuir integração com Active Directory para utilizar usuários e grupos de usuários na permissão de políticas e acessos, sem a necessidade de instalação de agente ou conector nos servidores de domínio.

QoS (Quality of Service)

A solução deve suportar o controle máximo ou garantido de largura de banda, em um endereço IP ou usuário específico;

A solução deve suportar o tunelamento com base no domínio de segurança, interface, endereço, usuários ou grupo de usuários, servidores ou pool, aplicativos ou pool de aplicativos;

A solução deve suportar largura de banda alocada por tempo, prioridade ou largura de banda compartilhada;

A solução deve suportar TOS e DiffServ;

A solução deve suportar políticas de QoS programadas para horários específicos;

A solução deve suportar a alocação de largura de banda com base na categoria de URL;

A solução deve suportar endereços IPv6 na função de QoS.

A solução deve suportar dois níveis de modelagem de tráfego que permitam modelagem de tráfego em diferentes dimensões, como usuários e aplicativos. A solução deve suportar pelo menos oito túneis por nível, o que proporciona uma hierarquia de controle de tráfego;

VPN

A solução deve suportar os seguintes recursos de VPN IPsec:

- Modo IPSEC Fase 1: modo de proteção agressivo e principal;
- IKEv1 e IKEv2 (RFC 4306);
- Método de autenticação: certificado e chave pré-compartilhada;
- DHCP sobre IPSEC;
- Fase 1 / Fase 2 de criptografia: DES, 3DES, AES128, AES192, AES256;
- Fase de Autenticação 1 / Fase 2: MD5, SHA1, SHA256, SHA384, SHA512;

A solução deve suportar VPN IPSec baseada em rotas e políticas;

A solução deve oferecer suporte Diffie-Hellman: 1,2,5;

A solução deve suportar os seguintes modos de implantação da VPN IPSEC: gateway-to-gateway, full-mesh, hub-spoke, túnel redundante, e modo transparente;

A solução deve possuir cliente de VPN SSL para Linux, iOS, Android e Windows, incluindo sistemas operacionais Windows de 64 bits;

A solução deve suportar SSL VPN com um único login que impede logins simultâneos com o mesmo nome de usuário;

A solução deve suportar verificação de integridade do host e verificação do sistema operacional antes da conexão do túnel SSL;

A solução deve suportar a opção de limpeza de cache antes de encerrar a sessão SSL VPN;

A solução deve suportar autenticação SSL com uma chave USB;

A solução deve suportar o modo de servidor e cliente L2TP, L2TP sobre IPSEC e GRE sobre IPSEC;

A solução deve suportar o PnPVPN para implantação rápida de várias filiais de VPN site-to-site.

Logs e Relatórios

A solução deve suportar a reversão do sistema operacional, ela deve suportar pelo menos duas cópias de firmware na memória flash do sistema;

A solução deve salvar dez versões do arquivo de configuração;

A solução deve suportar a exportação de configurações atuais e de backup para destinos externos, incluindo servidor FTP/ TFTP ou USB;

A solução deve suportar o SNMP;

A solução deve ser acessível através da interface gráfica (GUI) e da interface de linha de comando (CLI);

A solução deve suportar acesso ao gerenciamento de HTTP/HTTPS, SSH, Telnet e console;

A solução deve suportar pelo menos 3 funções de administrador, incluindo administrador, suporte ou operador e auditor ou reader;

A solução deve suportar a política de segurança de senha para contas de administrador;

A solução deve suportar armazenamento de logs localmente e em servidores syslog externos;

A solução deve suportar a transferência de logs sobre UDP e TCP;

A solução deve permitir que relatório possa ser exportado em PDF ou enviado por e-mail;

A solução deve suportar o RESTAPI.

Monitoramento

A solução deve apresentar estatísticas de tráfego de aplicativos e usuários;

A solução deve suportar o monitoramento de estatísticas para aplicativos, baseados em riscos, categorias, recursos e tecnologia;

A solução deve suportar estatísticas para visita de URLs e categorias URLs;

Deverá suportar estatísticas e análises de tráfego em tempo real;

Deverá suportar estatísticas de eventos de segurança;

Suporte para monitorar o status do dispositivo, como CPU, memória e temperatura;

Deverá ser possível acessar o equipamento a aplicar configurações durante momentos em que o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada;

Os relatórios podem ser exportados em formatos PDF ou HTML.

ITEM 2 - Solução para Gerenciamento de LOGS e Automação

A solução deve suportar blacklist de IP;

Suportar o recebimento de pacotes de contabilidade radius enviados por servidores de autenticação de terceiros, analisando informações on-line atuais do usuário;

Deve suportar a definição de regras de alarme para eventos de ameaça e operação do sistema, e disparar alarmes na forma de e-mails, mensagens de texto ou sons;

Deve suportar correlação de vários eventos de ameaças e configurar um mecanismo de kill chain para descobrir novas informações sobre ameaças e identificar com precisão os eventos de ameaças;

Deve suportar gerenciamento de nível hierárquico, permitindo conectar mais de uma plataforma e receber os logs na plataforma principal;

Deve suportar a análise de comportamento anormal e possuir banco de dados de modelo de comportamento de malware e base de conhecimento para análise baseada em honeypot;

Para total atendimento as especificações solicitadas, pode-se realizar composição com solução adicional, desde que não seja software livre. Caso a solução adicional não seja do mesmo fabricante da solução principal de firewall, deve possuir integração nativa entre as plataformas, e com ponto único de suporte;

A solução deve ter capacidade de armazenamento de logs de ameaças, sessões, tráfego, NAT, URL e outros, armazenando conforme o espaço em disco associado à appliance virtual de gerenciamento de logs;

Deve permitir rotacionar os logs conforme espaço de disco ocupado;

Deve suportar o envio de logs para servidor externo utilizando syslog;

Deve permitir a visualização de logs em tempo real;

Deverá ser instalada em ambiente virtual da CONTRATANTE, devendo estar disponível de forma local (on-site), em modelo virtual. Deve estar disponível para ambientes VMware ESXi e Hyper-V;

Deverá suportar coleta de dados, incluido Syslog para tratativa de logs em um ponto único central, sendo necesaria ter as seguintes capacidades;

Deve permitir investigação de logs, permitindo também para centralizar logs de terceiros na ferramenta;

Deve suportar o recebimento de logs dos próprios firewalls e de terceiros baseado em syslog;

Deverá unificar as ameaças reconhecidas pelo firewall ou fora dele, para rastreamento de eventos de ameaças com visualização de ativos de risco e tendências de risco;

Deve apresentar visualização distribuída de conexões geográficas de ameaças;

Deve suportar exibição em tela cheia de informações detalhadas e estatísticas para segurança geral, segurança de servidor, segurança de endpoint, e eventos de ameaças;

Deve permitir a criação de regras específicas para detecção de ameaças;

Deve suportar a coleta de evidências, processamento e marcação de status de eventos de ameaça;

Deve suportar a descoberta automática de ativos;

Deve apresentar informações sobre ameaças apresentando o CVE relacionado;

Deve permitir a criação de regras para detecção de ameaças específicas utilizando os logs recebidos dos firewalls e de terceiros;

Deve utilizar IA e ou ML para identificação de anomalias e comportamento anormal de tráfego;

Deve possuir banco de dados de inteligência de domínios DNS, códigos maliciosos, IP, vulnerabilidades, detecções de intrusão e geolocalização;

Deve suportat análise de killchain e integração com o MITRE ATT&CK para definição de técnica e tática;

Deve suportar pesquisa por palavras-chave, SPL e condições predefinidas nos logs recebidos;

A solução deve suportar REST API;

A solução deve suportar integração com o firewall ofertado neste projeto, para que possa automatizar os fluxos de resposta à incidentes detectados na rede;

Deverá possuir capacidade de criação de regras para automação de respostas, com regras pré-definidos e capacidade de criação de regras customizados através da interface gráfica;

A funcionalidade de automação, deverá ainda permitir que estas regras sejam utilizados para automação de respostas aos incidentes conforme configuração de gatilhos (triggers).

Essas triggers a serem usadas, podem ser eventos/características de ameaças, consulta de inteligência de ameaças, condições de julgamento para resposta automática e ações de processamento de resposta (políticas de emissão, bloqueio de IP ou criação de ordens de serviço), de modo a realizar resposta automática no firewall ou outro dispositivo.

Deve possuir painel que auxilie na visualização em tempo real de eventos de ameaças, sejam elas identificadas pelo firewall ou através de logs recebidos de outras fontes;

Deve suportar a geração de relatórios de ameaças e eventos;

Caso necessite de licenciamento adicional, deve cumprir no mínimo uma das seguintes métricas:

8000 (oito mil) eventos por segundo (EPS);

5000 (cinco mil) dispositivos.

ITEM 3 - Solução para Gerenciamento Centralizado de NGFW

A solução deve suportar a exibição de informações relacionadas, como nome do host do dispositivo, número de série do dispositivo, versão do software, plataforma de hardware, IP de gerenciamento, alarmes não tratados, versão do banco de dados de assinaturas, nova conexão e sessão;

Deve ser licenciada para a quantidade de 4 (quatro) appliances de firewall;

A solução deve suportar a exibição da utilização de CPU, utilização de memória, tráfego da máquina e outras informações do dispositivo em gráfico;

Deve permitir a criação de dashboards customizadas, apresentando minimamente informações de tráfego de aplicativos e usuários, além de informações sobre a saúde dos firewalls;

Deve permitir exportar logs de auditoria de configurações, contendo data/horário, ação e quem a executou;

A solução deve suportar a implantação rápida instalando automaticamente via USB (Zero Touch Provisioning);

O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

A solução deve suportar a troca de firmware do dispositivo firewall para uma versão salva localmente;

Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;

A solução deve suportar acesso remoto ao dispositivo via GUI e CLI;

A solução deve suportar o gerenciamento para configuração de roteamento dos dispositivos;

A solução deve suportar o gerenciamento de interfaces dos dispositivos;

A solução deve suportar reinicialização imediata do dispositivo e reinicialização programada;

A solução deve suportar o gerenciamento centralizado de firewall;

A solução deve suportar gerenciamento de estado de firewall e exibição de serviços;

A solução deve realizar a gestão de políticas globais de segurança para os firewalls;

A solução deve suportar o gerenciamento de configuração da política de segurança;

A solução deve suportar o gerenciamento de políticas de NAT de origem no dispositivo;

A solução deve suportar o gerenciamento de configuração de serviços e grupos de serviços;

A solução deve suportar o gerenciamento de configuração de aplicativos e grupos de aplicativos;

A solução deve suportar o gerenciamento de configuração do catálogo de endereços;

A solução deve suportar o gerenciamento de configuração de servidores AAA;

A solução deve suportar o gerenciamento de rótulos de recursos de aplicativos e grupos de recursos de aplicativos;

A solução deve suportar o gerenciamento de configuração de usuários locais;

A solução deve suportar o gerenciamento do modelo do sistema;

A solução deve suportar o gerenciamento do modelo de rede;

A solução deve suportar o gerenciamento de autorização de dispositivos;

A solução deve suportar atualização de versão do dispositivo;

A solução deve suportar atualização do banco de dados de assinaturas;

A solução deve suportar o gerenciamento do arquivo de configuração;

Deve apresentar ferramenta de diagnóstico de rede;

Deve permitir a criação de regras de alarmes para monitoramento de tráfego e recursos dos firewalls;

A solução deve permitir criação de política de senha, definindo critérios como complexidade e expiração;

Deve suportar alertas de hardware dos dispositivos;

Deve permitir o agrupamento de dispositivos por tipo e/ou por grupo;

O gerenciamento deve possuir recurso de comunicação via cliente ou web (GUI), utilizando protocolo seguro (criptografado), encriptação entre equipamento e sistema de gerenciamento;

Deve possuir mecanismo "Drill-Down" para visualização, em tempo real, das informações sumárias produzidas pela ferramenta de gerenciamento;

Deve suportar geração de relatórios contendo informações sobre o tráfego dos dispositivos de firewall;

Deve permitir que os relatórios possam ser exportados em PDF;

Deve exibir o volume de tráfego transferido nos túneis VPN;

Deve permitir a atualização dos firewalls de forma remota;

Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a de capacidade ilimitada.

ITEM 4 - CONFIGURAÇAO E INSTALAÇÃO

Uma vez entregue a solução, iniciar-se-á a etapa de instalação, com prazo máximo de 60(sessenta) dias, e compreenderá os seguintes procedimentos:

- A empresa vencedora procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos do CONTRATANTE, sendo posteriormente aferido e testado o seu perfeito funcionamento;
- A instalação deverá ocorrer nas dependências do MICD;
- Compreende-se, nesta etapa, a instalação de equipamentos, sistemas, softwares e aplicativos dos PRODUTOS fornecidos pela CONTRATADA, bem como a migração das configurações existentes na CONTRATANTE para os novos PRODUTOS;
- A migração das regras de segurança deverá ser realizada de forma automatizada, quando possível, com uso de software /script desenvolvido especificamente para este fim, com vistas a minimizar o impacto de um possível erro humano nas migrações de configurações.

A CONTRATADA deverá entregar os produtos de acordo com o ofertada em sua proposta e em absoluta conformidade com as exigências contidas neste documento.

Caso os produtos sejam diferentes dos propostos ou apresentem defeitos, serão automaticamente rejeitados; porém, a contagem do prazo de entrega não será interrompida em decorrência do produto rejeitado, arcando a CONTRATADA com o ônus decorrente desse atraso.

Os equipamentos devem ser novos, sem nenhum tipo de uso, entregues devidamente identificados e em conformidade com o exigido no edital e seus anexos, acondicionamento apropriado e demais itens complementares fornecidos pelo fabricante e em perfeitas condições para o uso, de forma a permitir completa segurança quanto à sua originalidade, sob pena do não recebimento do mesmo.

No ato da entrega dos equipamentos, deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos e instruções para instalação, configuração, operação e administração (quando aplicáveis), todos atualizados.

A documentação técnica poderá ser entregue em meio eletrônico, desde que seja em mídia oficial do fabricante.

O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do equipamento fornecido, cabendo-lhe sanar quaisquer irregularidades detectadas, quando da sua utilização durante o prazo da garantia

A CONTRATADA deverá entregar, instalar e configurar os equipamentos em até 60 (sessenta) dias consecutivos, podendo ser prorrogados por igual período após apresentação de justificativa e aprovação do MCID

O Recebimento provisório dar-se-á após instalação e configuração do equipamento, assim iniciando o período de avaliação do equipamento em termos de funcionalidades e performances, que darão embasamento para o recebimento definitivo.

3. Fundamentação e descrição da necessidade

Com a promulgação da Lei nº 14.600/2023, que deu origem ao Ministério das Cidades (MCID), mediante o desmembramento do Ministério do Desenvolvimento Regional (MDR), houve a necessidade de transferir competências e incumbências previamente atribuídas ao órgão extinto/transformado.

De acordo com o Decreto nº 11.468, de 5 de abril de 2023, o Ministério das Cidades (MCID) tem como áreas de competência os seguintes assuntos:

I - política de desenvolvimento urbano e ordenamento do território urbano;

II - políticas setoriais de habitação e de saneamento ambiental, incluídas as políticas para os pequenos Municípios e a zona rural;

III - política setorial de mobilidade e trânsito urbano;

IV - promoção de ações e programas de habitação e de saneamento básico e ambiental, incluída a zona rural;

V - promoção de ações e programas de urbanização, de desenvolvimento urbano, de transporte urbano e de trânsito;

VI - política de financiamento e subsídio ao desenvolvimento urbano, à habitação popular, ao saneamento e à mobilidade urbana;

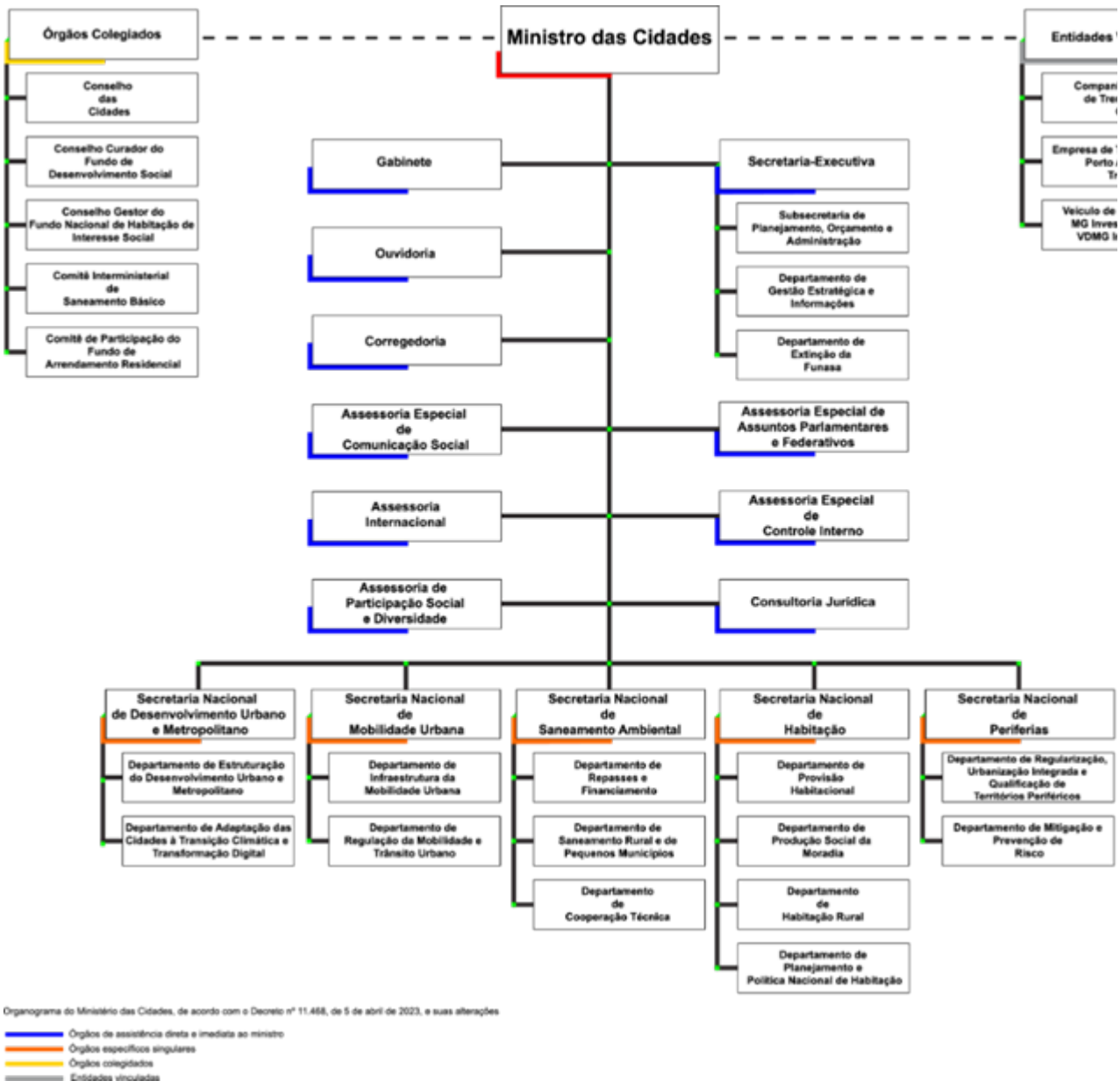
VII - planejamento, regulação, normatização e gestão da aplicação de recursos em políticas de urbanização, habitação e saneamento básico e ambiental, incluída a zona rural;

VIII - planejamento, regulação, normatização e gestão da aplicação de recursos em políticas de desenvolvimento urbano e de mobilidade e trânsito urbanos; e

IX - participação na formulação das diretrizes gerais para conservação dos sistemas urbanos de água e para adoção de bacias hidrográficas como unidades básicas do planejamento e da gestão do saneamento.

Atualmente a Estrutura Organizacional do Ministério das Cidades (MCID) compõe-se por:

ESTRUTURA ORGANIZACIONAL DO MCID



No âmbito governamental, a Tecnologia da Informação desempenha um papel fundamental na execução de políticas, no atendimento às demandas da população e na eficácia das operações.

Nesse contexto, torna-se imperativa uma seleção minuciosa de ferramentas tecnológicas que não devem apenas atender às necessidades imediatas, mas também criar um ambiente versátil, colaborativo e eficaz.

A Coordenação Geral de Tecnologia da Informação (CGTI) desempenha um papel essencial como provedor de tecnologias computacionais e sistemas de informação. Sua responsabilidade principal é oferecer soluções de informática eficientes e confiáveis, com o objetivo de aprimorar consideravelmente a qualidade dos serviços oferecidos à população. Adicionalmente, a CGTI é encarregada de gerenciar e supervisionar as iniciativas de informatização destinadas aos sistemas internos do Ministério das Cidades.

A Coordenação-Geral de Tecnologia da Informação (CGTI) é a responsável por desenvolver, aperfeiçoar, manter e dar suporte aos sistemas informatizados e aos bancos de dados no âmbito do MCID, administrando os recursos de informação e informática do órgão. Todas as áreas desse Ministério dependem de serviços específicos de Tecnologia da Informação para o desempenho de suas atividades.

As demandas da Tecnologia da Informação exigem métodos e ferramentas que garantam o nível de qualidade para atender às expectativas dos clientes e usuários, ao mesmo tempo em que acompanham a constante evolução de suas necessidades.

O presente documento analisa a contratação de uma solução composta por firewalls e suas respectivas ferramentas de gerenciamento e análise de logs, incluindo suporte e garantia. Esses ativos de segurança da informação são essenciais para a Coordenação-Geral de Tecnologia da Informação (CGTI) do Ministério das Cidades, pois permitem a gestão segura das atividades de proteção da infraestrutura contra ameaças e ataques cibernéticos, tanto da internet quanto de redes internas. Além disso, garantem acesso seguro, por meio de conexão VPN, aos servidores e colaboradores.

Atualmente, o MCID opera com uma infraestrutura de TI compartilhada com outros órgãos, como a FUNASA e o Ministério do Desenvolvimento Regional (MIDR). Cada órgão possui suas próprias particularidades e regulamentações, o que torna a situação desafiadora. A utilização de diferentes soluções de proteção de perímetro e equipes técnicas independentes dificulta a gestão de eventos de segurança e a resposta a incidentes, além de não permitir uma análise integrada dos dados.

Dessa forma, a criação de uma estrutura própria de proteção de perímetro é essencial para atender às demandas específicas do MCID, garantindo a implementação de políticas de segurança personalizadas e a proteção de dados sensíveis.

Além desta aquisição agregar tais benefícios, de acordo com a PORTARIA SGD/MGI Nº 852, DE 28 DE MARÇO DE 2023. O Programa de Privacidade e Segurança da Informação, o qual regulariza uma serie de processos e adequações em relação a privacidade e segurança da informação, esta aquisição também nos permite atender às diretrizes do PPSI como disposto no art. 3º e 4º do PPSI:

“CAPÍTULO II

DO PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Art. 3º O PPSI tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do SISP.

Art. 4º O PPSI caracteriza-se como um conjunto de projetos e processos distribuídos nas áreas temáticas de governança, maturidade, metodologia, pessoas e tecnologia.

§1º São iniciativas do PPSI:

I - definir e manter a estrutura de controles de privacidade e segurança da informação;

II - estabelecer e coordenar o Centro Integrado de Segurança Cibernética do Governo Digital - CISC Gov.br;

III - diagnosticar o grau de implementação dos controles de privacidade e segurança da informação pelos órgãos e entidades pertencentes ao SISP;

IV - acompanhar a implementação de controles e sensibilizar de forma contínua a Estrutura de Governança, prevista no art. 6º desta Portaria;

V - promover parcerias com órgãos e entidades públicas, entidades privadas e organismos internacionais para desenvolver e dar sustentação às iniciativas relacionadas ao tema, nos termos da legislação;

VI - promover as boas práticas por meio de disponibilização de guias, processos, modelos e procedimentos;

VII - estabelecer e coordenar o Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital;

VIII - promover a cultura de privacidade e segurança da informação;

IX - apoiar na prevenção, tratamento e resposta a incidentes cibernéticos; e

X - identificar e disseminar informações sobre vulnerabilidades para a prevenção, tratamento e resposta a incidentes cibernéticos.

§2º São valores do PPSI:

I - a maturidade;

II - a resiliência;

III - a efetividade;

IV - a colaboração; e

V - a inteligência.”

Com base na proposta de implementação de uma solução integrada de proteção de rede Next Generation Firewall (NGFW) no Ministério das Cidades (MCID), é possível avaliar se as medidas do Framework do Programa de Privacidade e Segurança da Informação (PPSI) serão atendidas. Abaixo está a avaliação de cada item listado:

Avaliação das Medidas do Framework do PPSI

O órgão implementa e gerencia um firewall nos servidores?

- **Avaliação:** Com a implementação de uma solução NGFW, essa medida será atendida, garantindo a proteção adequada dos servidores.

O órgão implementa e gerencia um firewall nos dispositivos de usuário final?

- **Avaliação:** A solução deve incluir capacidades de gerenciamento de segurança para dispositivos de usuário final, embora isso possa requerer soluções adicionais específicas.

O órgão executa a gestão automatizada de patches de aplicações?

- **Avaliação**: A solução NGFW deve ser capaz de suportar a gestão de patches, mas a implementação efetiva dependerá de processos internos já existentes.

O órgão retém os logs de auditoria?

- **Avaliação**: A aquisição da NGFW incluirá a capacidade de coletar e reter logs de auditoria, atendendo a essa exigência.

O órgão coleta logs de auditoria?

- **Avaliação**: A solução deve garantir a coleta de logs de auditoria, o que é uma função central da tecnologia.

O órgão coleta logs de auditoria detalhados?

- **Avaliação**: Espera-se que a NGFW permita a coleta de logs detalhados, conforme necessário para a segurança e a conformidade.

O órgão coleta logs de auditoria de consulta DNS?

- **Avaliação**: A funcionalidade deve estar presente na NGFW, permitindo a coleta de logs de consultas DNS.

O órgão coleta logs de auditoria de requisição de URL?

- **Avaliação**: A solução deve ser capaz de coletar logs detalhados de requisições de URL, garantindo visibilidade nas atividades de navegação.

O órgão coleta logs de auditoria de linha de comando?

- **Avaliação**: A coleta de logs de linha de comando pode depender de integrações adicionais, mas a solução deve facilitar essa necessidade.

O órgão centraliza os logs de auditoria?

- **Avaliação**: A solução NGFW deve permitir a centralização dos logs, melhorando a gestão de segurança e a análise de incidentes.

O órgão coleta logs do provedor de serviços?

- **Avaliação**: Isso dependerá de acordos com os provedores de serviços, mas a solução pode ser projetada para coletar esses logs.

O órgão implanta soluções para prevenção de intrusão baseada em host?

- **Avaliação**: A NGFW pode incluir funcionalidades de prevenção de intrusão, mas a proteção baseada em host pode exigir soluções complementares.

O órgão implanta soluções para prevenção de intrusão de rede?

- **Avaliação**: A solução NGFW atenderá a essa exigência, já que é projetada para prevenir intrusões na rede.

O órgão implanta soluções de detecção e intrusão baseada em host?

- **Avaliação**: Similar ao item 3.12.1.12., pode exigir soluções adicionais para proteção baseada em host.

O órgão implanta soluções de detecção e intrusão baseada em rede?

- **Avaliação**: A NGFW atenderá a essa necessidade, proporcionando detecção e resposta a intrusões na rede.

O órgão coleta logs de fluxo e tráfego de rede?

- **Avaliação**: A solução deve incluir a coleta de logs de fluxo e tráfego, garantindo visibilidade e análise.

O órgão treina desenvolvedores em conceitos de segurança de aplicações e codificação segura?

- **Avaliação**: Essa medida depende de programas internos de treinamento, que devem ser desenvolvidos em paralelo à implementação da solução.

O órgão aplica princípios de design seguro em arquiteturas de aplicações?

- **Avaliação**: A aplicação desses princípios deve ser parte do desenvolvimento de novas aplicações e sistemas.

O órgão aproveita os módulos ou serviços controlados para componentes de segurança de aplicações?

- **Avaliação**: Essa prática deve ser incorporada nas políticas de segurança, mas dependerá de uma estratégia mais ampla.

A organização, ao realizar registros de eventos (logs), considera o princípio de minimização de dados?

- **Avaliação**: A coleta de logs deve seguir diretrizes de minimização de dados, sendo essencial para conformidade com regulamentos de proteção de dados.

Nos últimos anos, a compreensão do valor dos dados como ativos intangíveis se intensificou, impulsionada pelo avanço tecnológico que transformou os processos de produção e armazenamento de informações. Para instituições como o Ministério das Cidades (MCID), que operam em ambientes cada vez mais conectados, a segurança da informação se torna uma prioridade. A utilização da Internet e de redes parceiras, embora traga oportunidades significativas de conectividade e lucro, também expõe as organizações a riscos consideráveis, incluindo infestações, adulteração, roubo de dados e ataques maliciosos.

O fluxo crescente de informações e a necessidade de disponibilização online de aplicações têm apresentado desafios significativos à segurança da informação e das comunicações no MCID. Com a crescente dependência de sistemas e serviços de informação, as ameaças cibernéticas se tornaram mais frequentes e sofisticadas, resultando em falhas de segurança que podem gerar prejuízos financeiros significativos, além de danos à reputação do Ministério.

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) responsável por coordenar as atividades de segurança da informação e das comunicações no governo federal, por meio da PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022,(https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918) deixa claro as orientações para proteção das entidades públicas do executivo federal, ao qual destacamos o item 2 e seu subitem 2.1:

“2. PREVENÇÃO

A prevenção é um processo constante de ações proativas com o objetivo de reduzir a probabilidade de ataques cibernéticos bem-sucedidos. Entre essas ações, enfatizam-se as de definição e de implementação de controles de segurança, de gerência mento de vulnerabilidades, de conscientização e de capacitação.

As ações preventivas de segurança cibernética deverão contemplar aquelas previstas na política de segurança da informação do integrante da Regic.

2.1. Definição e implementação de controles de segurança preventivos:

Os controles de segurança preventivos constituem-se em tecnológicos, organizacionais e físicos.

Os controles tecnológicos são aqueles utilizados para reduzir vulnerabilidades no hardware e no software. Entre os principais de controles tecnológicos estão:

- *dispositivos endpoint do usuário;*
- *restrição de acesso à informação;*
- *autenticação segura;*
- *proteção contra malware;*
- *backup das informações;*
- *atividades de monitora mento (log);*
- *segurança de redes;*
- *uso de criptografia; e*
- *gestão de mudanças.*

Por sua vez, os controles organizacionais são utilizados para assegurar a adequação contínua e efetiva da gestão de segurança da informação. Entre os principais controles organizacionais estão:

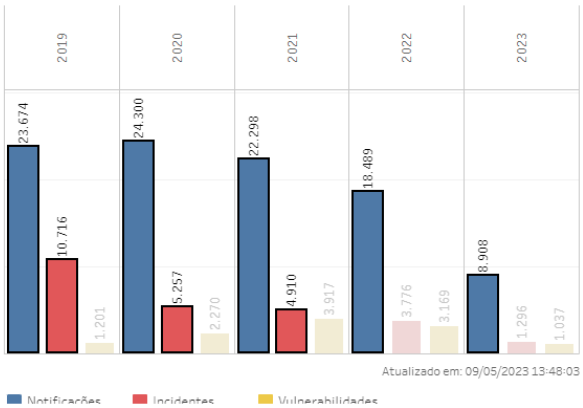
- *política de Segurança da Informação;*
- *definição de papéis e responsabilidades pela segurança da informação;*
- *segregação de funções;*
- *mapeamento de ativos de informação;*
- *controle de acesso;*
- *classificação e rotulagem de informações; e*
- *norma de segurança da informação para uso de serviços em nuvem.*

Por fim, os controles físicos têm por finalidade prevenir ou evitar o acesso não autorizado à área ou material sensível, bem como danos e interferências às áreas que contenham informações críticas ou sensíveis. Entre os principais controles físicos estão:

- *definição dos perímetros de segurança física;*
- *monitoramento de segurança física;*
- *proteção contra ameaças físicas e ambientais;*
- *localização e proteção de equipamentos;*
- *segurança de ativos fora das instalações da organização; e*
- *manutenção de ativos."*

Ainda nesta linha o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, entidade que está enquadrada na categoria "CSIRT de responsabilidade nacional de coordenação" publica regularmente relatórios sobre a quantidade de incidentes descobertos. Os dados podem ser acessados em https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral.

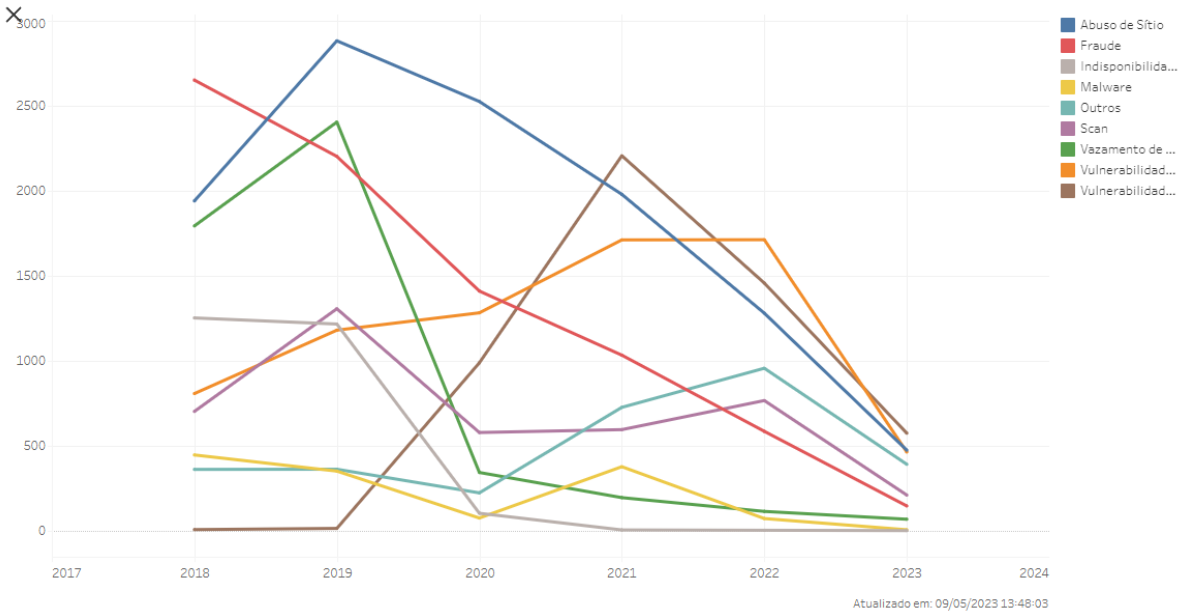
Abaixo, apresentamos as estatísticas das Notificações Reportadas e Incidentes/Vulnerabilidades Confirmados pelo CTIR Gov ao longo do tempo:



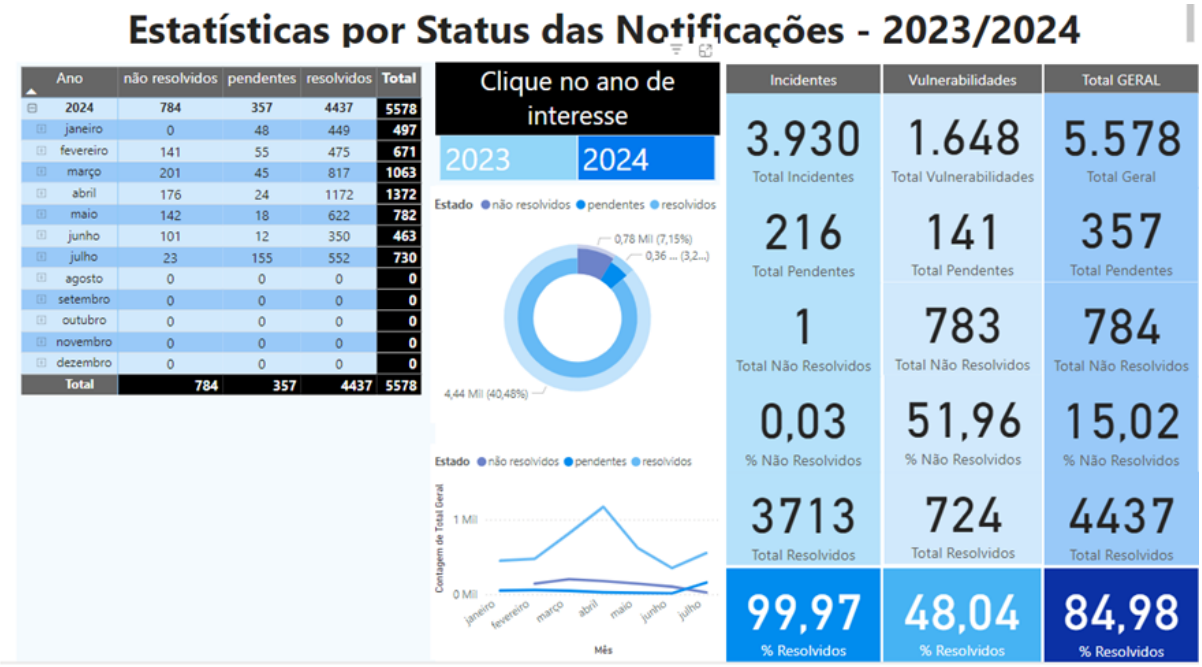
	2019	2020	2021	2022	2023
Notificações	23.674	24.300	22.298	18.489	8.908
Incidentes	10.716	5.257	4.910	3.776	1.296
Vulnerabilidades	1.201	2.270	3.917	3.169	1.037

Atualizado em: 09/05/2023 13:48:03

Com base nesses dados, a seguir está a Variação das Notificações por Categoria ao longo do tempo:



Para uma análise mais detalhada, apresentamos as estatísticas por status das notificações de 2023 e 2024:



Essas informações são essenciais para compreender a evolução dos incidentes cibernéticos e a efetividade das medidas de prevenção e resposta adotadas pelo CTIR Gov, permitindo uma avaliação crítica das ações implementadas e a identificação de áreas que necessitam de aprimoramento.

Adicionalmente, o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CSIRT) reporta um aumento significativo no número de incidentes de segurança cibernética no âmbito do governo federal. Em 2024, o volume de incidentes já superou o total de 2023, com um registro de 3.930 incidentes até o momento.

Neste contexto, a proteção de perímetros é uma das prioridades mais relevantes para a segurança institucional. As soluções de Next Generation Firewall (NGFW) oferecem um conjunto abrangente de funcionalidades para fortalecer a segurança da rede, adaptando-se continuamente às novas ameaças e vulnerabilidades.

Alinhamento aos Instrumentos de Planejamento Institucionais

O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

- ID PCA no PNCP: 05465986000199-0-000001/2024
- Data de publicação no PNCP: 07/08/2023
- Id do item no PCA: 81
- Classe/Grupo: 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA
- Identificador da Futura Contratação: 560010-13/2024

O objeto da contratação também está alinhado com a Estratégia de Governo Digital disponível no link (https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional), e em consonância com o Plano Diretor de Tecnologia da Informação - PDTI MIDR 2023/2026 (SEI nº 4781512), aprovado pelo Comitê de Governança Digital do Ministério das Cidades, em concordância com a Nota nº 00231/2023/CONJUR-MCID, e a consulta à Secretaria de Governo Digital do MGI.

Objetivos da Estratégia Nacional de Governo Digital para o período de 2024 a 2027:

OBJETIVO	**ID**	**RECOMENDAÇÃO**
4 - PRIVACIDADE E SEGURANÇA	4.1	Instituir estrutura de governança e coordenação para implementação de medidas de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, em articulação com estruturas de mesmo propósito de âmbito regional e nacional, em especial o Programa de Privacidade e Segurança da Informação – PPSI do governo federal.

4 - PRIVACIDADE E SEGURANÇA	4.2	Estabelecer plano de ação de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética que contemple diagnóstico, controles, metodologias e soluções tecnológicas adequadas aos riscos identificados.

Alinhamento ao Plano Diretor de Tecnologia da Informação - PDTI MIDR 2023/2026:

ALINHAMENTO AO PDTIC 2023-2026	
Id	**Ação**
NC04	Prover melhorias em soluções corporativas de TIC.
NC13	Prover soluções de segurança de TIC.
NC15	Prover infraestrutura de TIC.
A49	Adquirir Solução de Firewall.
A53	Soluções para teletrabalho seguro e gerenciável.

4. Requisitos da contratação

REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

A crescente complexidade e interconectividade dos ambientes digitais trazem desafios significativos à segurança da informação no Ministério das Cidades (MCID). Com o aumento do tráfego de dados e a crescente dependência de serviços online, proteger informações sensíveis e garantir a continuidade das operações se tornou uma prioridade estratégica. As principais necessidades do negócio que fundamentam a solução integrada de proteção de rede *Next Generation Firewall* (*NGFW*) são as seguintes:

1. Proteção de Dados Sensíveis: O MCID lida com informações confidenciais relacionadas a políticas públicas, habitação e infraestrutura. É crucial implementar medidas robustas para proteger esses dados contra acessos não autorizados e ciberataques.

2. Continuidade das Operações: A interrupção dos serviços pode ter consequências graves para a execução de políticas públicas e o atendimento à população. Um firewall eficaz garantirá a resiliência das operações, prevenindo e respondendo rapidamente a incidentes de segurança.

3. Conformidade Regulamentar: A aquisição de uma solução integrada de proteção de rede NGFW é necessária para atender às exigências estabelecidas por legislações e normas, como a PORTARIA SGD/MGI nº 852, que regula o Programa de Privacidade e Segurança da Informação (PPSI). Cumprir essas diretrizes é crucial para assegurar a integridade e a segurança das informações.

4. Integração e Gestão de Segurança: A atual infraestrutura de TI do MCID é compartilhada com outros órgãos, o que dificulta a gestão integrada da segurança. Uma solução NGFW própria permitirá implementar políticas de segurança personalizadas e aprimorar a coordenação nas respostas a incidentes.

5. Monitoramento e Análise em Tempo Real: A capacidade de monitorar e analisar logs de segurança em tempo real é essencial para identificar rapidamente ameaças e tomar decisões informadas. Isso é fundamental para a proteção proativa da infraestrutura digital do MCID.

6. Suporte à Inovação: À medida que o MCID adota novas tecnologias e serviços online, uma solução NGFW robusta proporcionará a segurança necessária para implementar essas inovações, permitindo que o ministério se adapte às demandas emergentes sem comprometer a segurança.

7. Cultura de Segurança da Informação: A adoção de uma solução NGFW ajudará a promover uma cultura de segurança dentro do MCID, educando os colaboradores sobre a importância da proteção de dados e do uso seguro de tecnologias.

Em suma, a aquisição de uma solução integrada de proteção de rede Next Generation Firewall (NGFW) é uma necessidade crítica para o MCID. Essa solução garantirá a proteção adequada de informações sensíveis, a continuidade das operações e a conformidade com as normativas, além de preparar o ministério para enfrentar os desafios da era digital.

Requisitos Legais

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) e a outras legislações aplicáveis;

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

Lei 12.305/ 2010 - Institui a Política Nacional de Resíduos Sólidos;

Decreto-Lei 200/67 - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

Decreto nº 7.174/10 - Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;

Resolução nº 717/2019 - Aprova o Regulamento de Qualidade dos Serviços de Telecomunicações – RQUAL;

Portaria SEGES/ME nº 8.678/2021 - Dispõe sobre a Governança das Contratações Públicas no âmbito da Administração Pública federal direta, autárquica e fundacional;

Instrução Normativa SEGES/ME nº 58, de 8 de agosto de 2022 - Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

Instrução Normativa SEGES/ME nº 81/2022 - Dispõe sobre a elaboração do Termo de Referência - TR, para a aquisição de bens e a contratação de serviços, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema TR digital;

Portaria GSI/PR nº 120, de 21 de dezembro de 2022 - que Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal;

Portaria SGD/MGI nº 852, de 28 de março de 2023 - que Dispõe sobre o Programa de Privacidade e Segurança da Informação - PPSI.

Requisitos de Manutenção

Devido às características da solução, há necessidade de realização de manutenções Preventiva e Corretiva pela Contratada, visando à manutenção da disponibilidade da solução.

Os requisitos de Manutenção seguem detalhados no item de Requisitos de Garantia, Manutenção e Assistência Técnica.

Requisitos Temporais

O prazo de vigência da contratação será de 60 (sessenta) meses contados da assinatura do contrato, na forma do artigo 105 da Lei n° 14.133, de 2021.

A reunião inicial de alinhamento com a Contratada, deverá ocorrer em no máximo 5 (cinco) dias corridos, posteriormente à assinatura do instrumento contratual.

Os bens/produtos devem ser entregues em até 45 (quarenta e cinco) dias corridos após a emissão da Ordem de Serviço ou de Fornecimento de Bens. Os bens/serviços entregues poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações ou critérios de aceitação, devendo ser substituídos às suas custas, sem prejuízo da aplicação das penalidades cabíveis. A instalação e configuração da solução devem ocorrer em até 60 (sessenta) dias.

A Contratada deverá cumprir todos os prazos descritos neste Termo de Referência, respeitando os prazos máximos estabelecidos e zelando pelo cumprimento dos Níveis Mínimos de Serviço Exigidos.

O prazo de início de atendimento para os chamados de suporte técnico e manutenção pela garantia deverá estar de acordo com o especificado no acordo de nível de serviço do Termo de Referência;

O prazo de entrega e instalação deverá estar de acordo com o especificado no Termo de Referência, caso não seja especificado um prazo diferente na ordem de serviço.

Os serviços e itens a qual se refere este projeto, devem ser entregues em Brasília.

A entrega deverá acontecer no horário compreendido entre as 09:00 as 17:00 e poderá ser agendada em data e hora previamente com a CONTRATANTE;

Caberá ao CONTRATANTE rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Termo de Referência.

O recebimento dos serviços e itens desse projeto, será efetivado pela equipe designada pelo CONTRATANTE, e dar-se-á da forma provisória e definitiva. A forma provisória será no ato da entrega dos equipamentos e a forma definitiva será após a instalação, configuração e teste da solução.

Requisitos de Segurança e Privacidade

Obedecer a todas as normas e procedimentos de segurança implementados no ambiente de TI do CONTRATANTE;

As pessoas envolvidas na execução das atividades terão acesso às instalações do CONTRATANTE por meio de credenciais emitidas pela Administração e deverão executar as atividades em ambiente definido pelo órgão, estando sujeitas, além do uso de crachás, a todas as formas de controle de acesso às dependências da instituição, tais como atendimento aos horários de expediente, vistoria de objetos que estejam portando etc.;

O acesso a áreas restritas, por técnicos das eventuais empresas CONTRATADAS, obedecerá ao previsto na POSIC do CONTRATANTE e suas Normas Complementares;

A execução das atividades deverá observar os princípios básicos de Segurança da Informação e Comunicações – SIC;

Além do que está descrito acima, deverão ser observados os requisitos de segurança e privacidade especificados nos requisitos tecnológicos da solução.

Requisitos Sociais, Ambientais e Culturais

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

Requisitos Sociais, como a responsabilidade social: a contratada deve demonstrar compromisso com a responsabilidade social, cumprindo as leis trabalhistas, respeitando os direitos humanos e adotando práticas éticas de negócios e a qualidade no atendimento: a contratada deve oferecer atendimento de qualidade, com prontidão nas respostas, comunicação eficaz, empatia e respeito aos usuários.

Requisitos Ambientais: Exige-se a que os profissionais realizem o uso eficiente de energia, práticas de descarte adequadas e conformidade com regulamentações ambientais aplicáveis.

Requisitos Culturais: Conhecimento da cultura e ambiente local: Consideração da compreensão da cultura local e dos desafios específicos da região, para garantir uma adaptação adequada dos serviços de TI à realidade do Ministério das Cidades (MCID).

Sensibilidade cultural: Avaliação da capacidade das empresas licitantes em lidar com a diversidade cultural e tratar os colaboradores e usuários com respeito e igualdade, promovendo um ambiente de trabalho inclusivo.

Requisitos de Arquitetura Tecnológica

A solução ofertada deverá observar integralmente os requisitos de arquitetura tecnológica descritos no item 2 deste Termo de Referência.

Requisitos de Projeto e de Implementação

A CONTRATADA deverá apresentar um Projeto Executivo, elaborado a partir do levantamento prévio da topologia, arquitetura e configuração atual do(s) ambiente(s) da CONTRATANTE. Esse projeto deve ser composto por um documento do tipo SOW (em tradução livre, escopo de trabalho) e conter, no mínimo, as seguintes informações:

- Objetivo;
- Plano de gerenciamento de mudanças, detalhando passo a passo o escopo da migração;
- Cronograma das atividades que serão realizadas, com os prazos estimados, considerando o cronograma de execução proposto neste Termo e as diretrizes para cada atividade;
- Projeto lógico de configuração e diagrama de interconexão dos equipamentos;
- Nome(s) do(s) gerente(s) de projeto e do(s) técnico(s) responsável(is) pela execução;
- Lista de todos os elementos instalados, contendo:
    - Nome e endereço(s) IP do equipamento;
    - Equipamento e porta na qual o equipamento foi conectado;
    - Local de instalação (prédio, andar, sala);
    - Número de série do equipamento.
- A instalação refere-se à instalação física e lógica nos locais indicados pela CONTRATANTE, abrangendo também:
    - Sua disposição e conectorização no rack de telecomunicações;
    - A instalação dos transceivers em seus módulos/slots;
    - Sua interconexão aos switches, roteadores, ADCs e servidores de rede, entre outros;
    - Suas configurações de interfaces, endereçamento e serviços de rede, além de outras configurações necessárias ou constantes no Projeto de Instalação;
    - Sua identificação e a identificação de todas as suas conexões.

O SOW deverá ser entregue pela CONTRATADA em até 10 (dez) dias úteis após a assinatura do contrato, o qual deverá ser aprovado pela CONTRATANTE. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes. O Projeto deverá ser elaborado pela CONTRATADA após a abertura da Ordem de Serviço, em tempo hábil para ser validado e aprovado pela equipe de fiscalização do contrato, considerando os prazos previstos no item de cronograma de execução.

As reuniões de controle do projeto deverão ser documentadas e registradas em ata, com as assinaturas dos presentes ou gravadas quando realizadas on-line. A data e a periodicidade de realização serão definidas em comum acordo entre as partes envolvidas no contrato.

Caberá ao Gerente de Projetos da CONTRATADA a responsabilidade por elaborar e apresentar ao CONTRATANTE os relatórios de progresso da execução contratual, bem como relatar todas as situações pertinentes à situação do projeto, incluindo a relação de atividades executadas no período, pendências e solicitações de mudança no cronograma do projeto, entre outros assuntos relacionados. Os relatórios de progresso (relatórios de acompanhamento) deverão ser disponibilizados ao CONTRATANTE em data e/ou periodicidade a ser definida em comum acordo entre as partes.

Requisitos de Implantação

A CONTRATADA deverá observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

A instalação e configuração deverão ser executadas por técnicos da CONTRATADA, certificados pelo fabricante dos equipamentos fornecidos. É necessária a apresentação de documentação original que comprove a validade dessas certificações enquanto durar o contrato, podendo ser solicitada a qualquer momento.

Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, que podem ser realizadas presencialmente, por telefone ou via conferência web. A CONTRATADA deverá sugerir as configurações de acordo com normas e boas práticas, cabendo à CONTRATANTE a aceitação expressa ou recusa nos casos de não atendimento às condições estabelecidas.

As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE. A CONTRATADA deverá analisar o ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo a garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet etc.).

A substituição da infraestrutura de firewall instalada no local deve ser planejada e executada de modo a não causar interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE. Caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante uma janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados. Deverão ser realizadas as seguintes atividades mínimas:

- Instalação física, cabeamento e adaptações elétricas necessárias para interligação ao sistema nos datacenters da CONTRATANTE, acompanhadas e aprovadas pelas equipes técnicas responsáveis do CONTRATANTE;
- Configuração inicial do sistema, incluindo configuração de acesso de gerenciamento (usuários e senhas), configuração inicial de rede, configuração de monitoramento e ativação de licenças de criptografia e outras necessárias;
- Atualização de firmware/drivers da solução;
- Demais atividades necessárias para o perfeito funcionamento do sistema.

Todo o trabalho referente ao cabeamento, quando necessário, deverá ser realizado atendendo às normas técnicas aplicáveis, incluindo a adequada organização e identificação de cabos, segundo padrão de qualidade já existente. Todos os aspectos relacionados à adequação das condições elétricas e de rede de dados necessários à instalação dos equipamentos deverão ser levantados durante a vistoria. Durante esta etapa, as licitantes deverão avaliar os detalhes técnicos necessários ao cumprimento de suas obrigações. A adequação ao ambiente deverá englobar o fornecimento/substituição de todos os cabos, conectores, guias, leitos aramados, tomadas, abraçadeiras, velcros e demais componentes necessários à interligação de todos os produtos de hardware ofertados.

Todos os cabos e conectores fornecidos deverão ser certificados por órgãos competentes e deverão possuir o comprimento adequado para interligar todos os equipamentos fornecidos. Os equipamentos de rack deverão ser instalados nos racks disponíveis nas dependências do datacenter do CONTRATANTE. Caso haja necessidade de instalação de rack proprietário ou de adaptador para instalação em rack padrão, este deverá ser fornecido pela CONTRATADA, que providenciará todos os ajustes necessários no datacenter para que o equipamento seja devidamente instalado. Caberá à empresa CONTRATADA a conexão dos cabos aos demais equipamentos. Todo cabeamento deve ficar devidamente organizado e identificado com etiquetas apropriadas, fornecidas pela CONTRATADA.

O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares necessários à instalação, é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus adicionais ao CONTRATANTE.

A falta de peças ou equipamentos não será considerada como alegação de força maior e não eximirá a CONTRATADA das penalidades a que estará sujeita pelo não cumprimento dos prazos estabelecidos. A CONTRATADA deverá atuar, sempre que solicitado, em qualquer movimentação de equipamentos no datacenter – entre espaços e racks, dentro do ambiente do CONTRATANTE e fora deste, conforme necessário.

A CONTRATADA deverá manter o local de execução dos serviços em perfeitas condições de limpeza e uso.

O Gerente de Projetos da CONTRATADA deverá, após a implantação da solução (instalação e configuração), entregar a documentação de “as built” em meio eletrônico, contendo todas as informações relativas à instalação e configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização, de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento.

Deverá constar da documentação de “as built” todas as informações do Projeto Executivo atualizadas, como a localização física no datacenter da CONTRATANTE, conexões físicas utilizadas, endereços IP e nomenclaturas, onde deverão ser demonstradas as velocidades e a qualidade da transmissão de dados.

A entrega da documentação de “as built” sinaliza a conclusão da etapa de implantação, solicitando a validação para fins de recebimento definitivo. Esta documentação também deverá conter fotos do ambiente instalado, assim como, se necessário, imagens ilustrativas de configurações.

Requisitos de Garantia, Manutenção e Assistência Técnica

O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

A garantia será prestada com o objetivo de manter os equipamentos e itens de software fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o CONTRATANTE.

A garantia abrange a realização da Manutenção Preventiva e Corretiva dos bens, realizada pelo próprio CONTRATADO ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

Entende-se por Manutenção Preventiva os serviços que compreendem verificações frequentes em relação ao bom funcionamento do hardware e à atualização de drivers, softwares e firmwares necessários para todos os itens que compõem os equipamentos. Quando necessário, haverá a substituição de peças e componentes, que deverão ser novos, originais e não recondicionados. Os serviços deverão ser realizados mediante cronograma de execução previamente aprovado pelo CONTRATANTE.

As verificações preventivas ocorrerão pelo menos trimestralmente, em datas a serem definidas pelo CONTRATANTE. A manutenção preventiva poderá ser solicitada pela CONTRATANTE, que definirá o nível de severidade, por meio de chamado registrado junto à CONTRATADA.

A CONTRATADA deverá emitir um relatório de atendimento de manutenção preventiva, que deverá evidenciar os parâmetros de desempenho do equipamento, as versões de software e as recomendações, quando for o caso.

Uma vez identificados vícios ou defeitos nos equipamentos, a CONTRATADA deve prover todas as manutenções corretivas necessárias para a normalização do ambiente, corrigindo todos os defeitos, mensagens de erro ou qualquer tipo de mau funcionamento apresentado em qualquer um dos equipamentos e seus componentes internos.

Entende-se por Manutenção Corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos, atualizações e correções necessárias.

As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento, sem custo adicional para o CONTRATANTE.

Uma vez notificado, o CONTRATADO realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo máximo de 1 (um) dia útil, contados a partir da data de retirada do equipamento das dependências da Administração pelo CONTRATADO ou pela assistência técnica autorizada.

O prazo indicado no subitem anterior poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do CONTRATADO, aceita pelo CONTRATANTE.

Na hipótese do subitem acima e seu predecessor, o CONTRATADO deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo CONTRATANTE, de modo a garantir a continuidade dos serviços e trabalhos administrativos durante a execução dos reparos.

Decorrido o prazo para reparos e substituições, ou violados os NÍVEIS MÍNIMOS DE SERVIÇO, sem o atendimento da solicitação do CONTRATANTE ou a apresentação tempestiva de justificativas pelo CONTRATADO, fica o CONTRATANTE autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do CONTRATADO o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do CONTRATADO.

A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo a eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

Requisitos de Experiência Profissional

Os serviços de Garantia, Manutenção e Assistência Técnica deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

A CONTRATADA deverá possuir equipe qualificada para realizar:

- A instalação e configuração dos equipamentos e/ou licenças de software previstos na presente contratação;
- A execução da assistência técnica, manutenção e garantia, nos casos em que deverá efetuar manutenção corretiva, cobrindo todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias, quando for o caso.

Outros requisitos estão estabelecidos nos itens de requisitos de Garantia, Manutenção e Assistência Técnica e de Qualificação Técnica para Habilitação.

Requisitos de Formação da Equipe

Os serviços deverão ser prestados por técnicos devidamente capacitados.

Todos os recursos humanos necessários à realização das atividades de instalação e configuração da solução estão sob responsabilidade da CONTRATADA e serão supervisionados pela CONTRATANTE.

Deverá ser apresentado um Preposto, nos termos do art. 118 da Lei 14.133/2021, aceito pela Administração, para representar a CONTRATADA ao longo da execução do contrato.

Deverá ser apresentado um Gerente de Projetos (podendo este ser o Preposto), que será o ponto focal para tratativas de assuntos relativos à execução dos serviços, sendo responsável por coordenar e orientar todos os técnicos na execução dos serviços, de forma que os prazos e a qualidade estabelecidos sejam respeitados. Caberá ainda ao Gerente de Projetos apresentar na reunião uma lista de contatos para comunicação, a fim de esclarecer dúvidas ou oferecer apoio em itens relacionados ao projeto.

Requisitos de Metodologia de Trabalho

O fornecimento dos equipamentos está condicionado ao recebimento, pelo CONTRATADO, de uma Ordem de Serviço ou de Fornecimento de Bens (OSFB) emitida pela CONTRATANTE. A OSFB indicará o tipo de equipamento, a quantidade e a localidade onde os equipamentos deverão ser entregues. O CONTRATADO deve fornecer meios digitais para contato e registro de ocorrências relacionadas aos serviços de Garantia, Manutenção e Assistência Técnica, com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana.

O andamento do fornecimento dos equipamentos deverá ser acompanhado pelo CONTRATADO, que dará ciência à CONTRATANTE sobre eventuais acontecimentos. A CONTRATANTE será responsável pela condução da metodologia de trabalho. A CONTRATADA deverá adotar as boas práticas e técnicas conhecidas de gerenciamento de projeto.

Os produtos e/ou serviços deverão ser entregues no endereço indicado no item de “Entrega”, em prazo não superior ao que for definido neste Termo. Os equipamentos e as licenças de software serão instalados e configurados pela equipe técnica da CONTRATADA.

Os Fiscais Técnico e Requisitante emitirão um Termo de Recebimento Provisório quando da entrega do objeto resultante de cada Ordem de Serviço ou de Fornecimento de Bens. Após a instalação e configuração dos equipamentos e/ou softwares e das respectivas licenças pela CONTRATADA, e após a análise da qualidade e verificação da aderência aos termos contratuais pelos Fiscais e pelo Gestor do Contrato, o CONTRATANTE emitirá um Termo de Recebimento Definitivo dos produtos.

O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato. Será realizado o acompanhamento do contrato pela Equipe de Gestão e Fiscalização Contratual, inclusive nos casos de necessidade de manutenção e garantia da CONTRATADA.

O não cumprimento dos prazos exigidos ensejará sanções previstas no Termo de Referência.

Requisitos de Segurança da Informação e Privacidade

Os serviços prestados deverão estar em conformidade com as leis, normas e diretrizes vigentes no âmbito da Administração Pública Federal, especialmente no que tange à Segurança da Informação e Comunicações (SIC) e à Lei Federal nº 13.709/2018 (LGPD).

Conformidade com Normas e Políticas:

A CONTRATADA deverá adotar a Política de Segurança da Informação e Comunicações (POSIC) do Ministério das Cidades, além das normas federais relacionadas à segurança da informação.

Credenciamento e Seleção de Profissionais:

A CONTRATADA deverá credenciar junto à CONTRATANTE todos os profissionais designados para a execução dos serviços, independentemente do formato de trabalho (presencial, remoto ou híbrido).

Além disso, a CONTRATADA deverá aplicar critérios rigorosos no processo seletivo, garantindo que os profissionais designados não comprometam a segurança ou a credibilidade da CONTRATANTE.

Gestão de Acesso:

A CONTRATADA deverá informar à CONTRATANTE, com antecedência mínima, sobre qualquer alteração nos quadros de funcionários envolvidos na execução do contrato (transferência, remanejamento ou demissão), a fim de revogar imediatamente os acessos aos sistemas e informações da CONTRATANTE.

Identificação e Confidencialidade:

Os funcionários da CONTRATADA envolvidos na prestação de serviços deverão utilizar crachás de identificação.

Todas as informações acessadas pela CONTRATADA durante a execução dos serviços deverão ser tratadas como confidenciais, sendo proibida sua reprodução, utilização ou divulgação sem a devida autorização.

Sigilo e Proteção de Dados:

A CONTRATADA, seus representantes e colaboradores deverão garantir a confidencialidade de dados, informações, documentos e especificações técnicas adquiridas no desempenho das atividades. Além disso, a CONTRATADA deve implementar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações tratadas.

Prevenção de Acesso Não Autorizado:

A CONTRATADA deverá adotar medidas preventivas para proteger os dados, antecipando ameaças à segurança e à privacidade, e evitando acessos não autorizados às informações compartilhadas para a execução dos serviços.

Proibição de Transferência de Dados:

A CONTRATADA está proibida de obter, copiar ou transferir qualquer informação de propriedade da CONTRATANTE sem a devida autorização.

Cumprimento de Normas de Segurança:

A CONTRATADA deverá seguir os procedimentos estabelecidos nas normas de segurança corporativa do Ministério das Cidades (MCID) e da Administração Pública, em todos os eventos em que for necessária a presença de seus representantes nas dependências da CONTRATANTE.

Identificação de Equipamentos:

Qualquer equipamento da CONTRATADA instalado nas dependências da CONTRATANTE deverá ser devidamente identificado, utilizando placas de controle patrimonial, selos de segurança ou outros meios adequados.

Termos de Compromisso e Ciência:

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

- Anexo lll - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (SEI nº 5374352);
- Anexo II - TERMO DE CIÊNCIA (SEI nº 5374344).

Sustentabilidade

Devem ser atendidos os seguintes requisitos de sustentabilidade, conforme estabelecido no Guia Nacional de Contratações Sustentáveis:

Só será admitida a oferta de Next Generation Firewall(NGFW) que cumpra os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 304, de 2023 do INMETRO.

Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021):

Na presente contratação, não será admitida a indicação da marca/fabricante;

Da exigência de carta de solidariedade

Em caso de fornecedor revendedor ou distribuidor, não será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato.

Subcontratação

Não é admitida a subcontratação do objeto contratual.

Da verificação de amostra do objeto

Não será exigida a verificação de amostra do objeto

Garantia da Contratação

Será exigida a garantia da contratação a que se referem os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e nas condições descritas nas cláusulas do contrato.

Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-lo, no máximo, até a data de assinatura do contrato.

A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

O contrato poderá oferecer maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

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

A proposta de preços deverá ser apresentada de acordo com o Modelo de Proposta de Preço (Anexo II - SEI nº 5374204). A proposta de preços deverá ser apresentada com descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas neste Termo de Referência e no Edital.

A proposta técnica de preços deverá ter prazo de validade não inferior a 60 (sessenta) dias corridos, a partir da data da sessão pública.

A licitante deverá declarar, no momento de sua proposta, que possui capacidade técnica adequada para executar o objeto da licitação atendendo aos critérios de qualidade e aos níveis de serviço exigidos, cumprindo os requisitos especificados para a presente contratação.

A proposta deverá ser redigida em Língua Portuguesa (pt-BR), salvo quanto às expressões técnicas de uso corrente, sem emendas, rasuras ou entrelinhas, devidamente datada, sendo clara e precisa, sem alternativas de preços ou qualquer outra condição que induza o julgamento a ter mais de um resultado, com todos os preços expressos em REAIS (R$) e declaração expressa de que os serviços ofertados atendem aos requisitos técnicos especificados no Termo de Referência.

5. Papéis e responsabilidades

PAPÉIS E RESPONSABILIDADES

São obrigações da CONTRATANTE:

nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos, cuja criação ou alteração seja, objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

São obrigações do CONTRATADO:

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

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

reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

manter, durante toda a execução do contrato, as mesmas condições da habilitação;

quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

fazer a transição contratual, quando for o caso;

A CONTRATADA deverá disponibilizar a solução em conformidade com nível de serviço;

A CONTRATADA deverá disponibilizar logs e dados detalhados de transações de usuários na solução por um período mínimo de 120 dias;

A CONTRATADA deverá possuir política de atualização/migração de versão do software/aplicação em sua infraestrutura;

A CONTRATADA deverá ter Política de Backup compatível com a Política de Cópia de Segurança;

A solução da CONTRATADA deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, sem interrupção fora do horário comercial ou em finais de semana e feriados;

A Contratada deverá manter backup atualizado da base de dados;

Entregar a lista de profissionais com **TERMO DE CIÊNCIA** a critério da CONTRATANTE.

6. Modelo de execução do contrato

MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

O gestor do contrato emitirá a Ordem de fornecimento de bens ou Ordem de Serviço (OFB/OS) para a entrega dos bens e serviços desejados.

O CONTRATADO deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB e serviços com a qualidade mínima especificada neste Termo e definida na OS.

O recebimento provisório e definitivo é disciplinado em tópico próprio deste TR.

Forma de execução e acompanhamento do contrato

O acompanhamento e a fiscalização da execução dos contratos consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, conforme se depreende da Lei 14.133, de abril de 2021;

A verificação da adequação da prestação do serviço e da entrega dos bens deverá ser realizada com base nos critérios previstos neste Termo de Referência;

A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 33 da IN nº 94/2022;

A utilização dos meios apresentados neste Termo de Referência não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços;

Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas;

O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizados;

Em hipótese alguma será admitido que a própria CONTRATADA realize a avaliação de desempenho e qualidade da prestação dos serviços;

A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador;

Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas sanções à CONTRATADA de acordo com as regras previstas no ato convocatório;

O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposições da Lei nº 14.133, de 1º de abril de 2021.

Condições de Entrega

Os bens/produtos devem ser entregues em até 45 (quarenta e cinco) dias corridos após a emissão da Ordem de Serviço ou de Fornecimento de Bens. Os bens/serviços entregues poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações ou critérios de aceitação, devendo ser substituídos às suas custas, sem prejuízo da aplicação das penalidades cabíveis. A instalação e configuração da solução devem ocorrer em até 60 (sessenta) dias.

Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas, com a devida comprovação, com pelo menos 24 (vinte e quatro) horas de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

A entrega dos equipamentos será nas unidades do Ministério das Cidades em Brasília-DF. Antes do envio dos equipamentos, a Contratada deverá confirmar com o Contratante o endereço completo da entrega e instalação.

A Contratada deverá informar à Contratante sobre a entrega dos equipamentos com, no mínimo, 5 (cinco) dias de antecedência, ficando a Contratada responsável pelo transporte e entrega dos equipamentos.

Formas de transferência de conhecimento

O repasse de conhecimento trata-se de explanação teórica e prática para administradores da solução adquirida.

O repasse de conhecimento poderá ser remoto ou a **CONTRATANTE** disponibilizará em seu ambiente uma sala para a execução do repasse, com infraestrutura e apoio básicos (mesas, cadeiras, projetor, tela de projeção, computadores); em caso de impossibilidade de realização no ambiente da **CONTRATANTE**, caberá à **CONTRATADA** arcar com toda a infraestrutura (salas, instalações e equipamentos, recursos audiovisuais etc.).

O repasse de conhecimento deverá abordar procedimentos de instalação física e lógica;

Procedimentos necessários à configuração técnica e à completa operação do produto;

Procedimentos de manutenção do produto;

Apresentação geral da solução fornecida;

Descrição detalhada das partes e componentes de toda a solução, apresentando suas características funcionais;

Outros tópicos da solução necessários ao pleno domínio da solução e suas Integrações poderão ser explanados em comum acordo entre as partes na Reunião Inicial de Projeto.

O repasse de conhecimento deverá contemplar operação, Configuração e Administração da Solução ofertada em um prazo máximo de até 30 (trinta) dias após a instalação para toda a equipe indicada pela CONTRATANTE**.**

A CONTRATADA deverá providenciar todo o material didático individual que abranja todo o conteúdo necessário. Não será exigido material oficial do fabricante, entretanto este conteúdo será avaliado pela equipe do CONTRATANTE antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pelo CONTRATANTE.

Ao término do repasse de conhecimento a CONTRATADA deverá providenciar certificado de conclusão aos participantes contendo no mínimo nome do curso, carga horária, nome do concluinte, nome e logo da instituição que ministrou o curso.

SUPORTE 24X7

Os serviços de suporte técnico deverão contemplar as manutenções corretivas e evolutivas para a solução contratada e não poderão acarretar custos adicionais ao CONTRATANTE, além do contratado, durante todo o período de 60 (sessenta) meses. Ou seja, a CONTRATADA deverá declarar expressamente que se responsabilizará pelo pleno funcionamento, mantendo a solução em operação.

Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada.

Os serviços de suporte técnico deverão ser prestados em regime 24x7, ou seja, 24 horas por dia todos os dias do ano, e deverão ser realizados da seguinte forma:

Suporte Remoto – serviço de atendimento aos chamados técnicos, executados por meio telefônico, web ou e-mail, via central de help desk, em período integral, que tratará da abertura de chamados técnicos e ocorrências relativas à solução;

Suporte On-Site – No qual, deverá a CONTRATADA, disponibilizar de um recurso alocado in-loco na estrutura da CONTRATANTE, de forma dedicada em caráter 8/5, durante a vigência contratual.

Em todo atendimento técnico solicitado deverá ser fornecido o número do chamado na sua abertura bem como o responsável pela abertura e os motivos ou problemas referentes ao chamado;

Para a execução de atendimento, é necessária a autorização da CONTRATANTE para instalação ou desinstalação de quaisquer softwares ou componentes;

Todos os técnicos de suporte da CONTRATADA devem ser capacitados e certificados, pelo fabricante dos produtos a prestar atendimento de suporte técnico;

Ainda poderão ser executadas as seguintes tarefas em relação à prestação de suporte: resolução de dúvidas sobre o produto, discussão de melhorias na configuração, ativação de funcionalidades, ativação/desativação e manutenção de links tronco (DDR) em conjunto com operadora contratada pela CONTRATANTE, e resolução de pequenos problemas e ajustes na solução;

Os chamados técnicos serão sempre realizados pela CONTRATANTE, diretamente à CONTRATADA que, no caso de ter Assistência Técnica Terceirizada, deverá tomar todas as providências necessárias ao pleno atendimento do chamado junto à sua credenciada, obedecendo rigorosamente os prazos e condições aqui estabelecidos.

Todos os componentes destinados à reparação dos produtos em manutenção deverão ser novos e originais, com garantia co-terminus.

A CONTRATADA deverá manter o serviço de suporte técnico, disponível para a abertura e acompanhamento de chamados em tempo integral, 24 (vinte e quatro) horas por dia todos os dias do ano, inclusive sábados, domingos e feriados, com início de atendimento e prazo de solução de acordo com o nível mínimo de serviço e de severidade exigido para o caso, conforme os índices de criticidade abaixo:

SEVERIDADE	**DESCRIÇÃO**	**1 º ATENDIMENTO**	**SOLUÇÃO PALIATIVA**	**SOLUÇÃO DEFINITIVA**
		PRAZOS EM TEMPO CORRIDO A PARTIR DA NOTIFICAÇÃO		
Crítica	Sistema parado ou produto inoperante com impacto direto nas operações críticas de negócio. Aplicado quando há a indisponibilidade total ou frequente da solução.	02 (duas) horas	04 (quatro) horas	06 (seis) horas
Alta	Alto impacto no ambiente de produção ou grande restrição de funcionalidade com instabilidade no funcionamento da solução, perda de redundância ou impossibilidade de efetuar novas configurações ou diagnósticos.	04 (quatro) horas	08 (oito) horas	12 (doze) horas
Média	O defeito não gera impacto ao negócio, ocorre quando há indisponibilidade de alguma funcionalidade da solução ou ocorrência de evento causando impacto limitado.	04 (quatro) horas	08 (Oito) horas	24 (Vinte e Quatro) horas
Baixa	Aplicado para a instalação, configuração, upgrade, update e esclarecimentos técnicos relativos ao uso e aprimoramento do software.	08 (Oito) horas	12 (Doze) horas	72 (Setenta e duas) horas

Procedimentos de transição e finalização do contrato

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

Descredenciamento da equipe técnica da contratada;

Transferência de credenciais de acesso;

Elaboração de relatório final com as atividades realizadas durante o contrato;

Assinatura do Termo de encerramento contratual.

Quantidade mínima de serviços para comparação e controle

Cada OS conterá o volume de serviços demandados, incluindo a sua localização e o prazo, conforme modelo descrito no Anexo IV - MODELO DE ORDEM DE SERVIÇO (SEI nº 5374368).

Mecanismos formais de comunicação

O canal de comunicação entre a CONTRATANTE e CONTRATADA, para assuntos relacionados à gestão e fiscalização contratual, ocorrerá preferencialmente através da figura do preposto.

Como instrumentos de comunicação oficial entre a CONTRATANTE e a CONTRATADA, serão utilizados, no mínimo, os que seguem:

Ofícios;

E-mail;

Ordem de serviço;

Relatório Geral de Faturamento;

Termo de recebimento provisório;

Termo de recebimento definitivo;

Ata de reunião;

Serviços de Mensagens Oficiais (Exemplo MS Teams);e

Termo de Encerramento do Contrato

Formas de Pagamento

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

Manutenção de Sigilo e Normas de Segurança

A CONTRATADA 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.

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 da CONTRATADA, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos ANEXOS II (SEI nº 5374344) e III (SEI nº 5374352).

7. Modelo de gestão do contrato

MODELO DE GESTÃO DO CONTRATO

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.

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.

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

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

Reunião Inicial

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.

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 5 (cinco) dias após assinatura do contrato, podendo ser prorrogada a critério da CONTRATANTE.

A pauta desta reunião observará, pelo menos:

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

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

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

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.

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

Fiscalização

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

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);

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);

Identificada qualquer inexatidão 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);

O fiscal técnico do contrato informará ao gestor do contato, 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).

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).

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

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).

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

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).

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).

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).

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).

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).

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).

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.

Critérios de Aceitação

A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionadas por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Procedimentos de Teste e Inspeção

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

Após a implantação da solução (Itens 1, 2 e 3):

Verificação de conformidade dos requisitos especificados e da instalação e configuração, incluindo a entrega da documentação.

Após a realização do treinamento (transferência de conhecimento):

Verificação de conformidade dos requisitos de transferência de conhecimento.

Níveis Mínimos de Serviço Exigidos

Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	***Descrição***	
Finalidade	*Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.*	
Meta a cumprir	***IAE <= 0***	*A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.*
Instrumento de medição	Registro de assinatura de Ordem de Serviço ou de Fornecimento dos Bens – OSFB e seus respectivos Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	*A avaliação será feita conforme linha de base do cronograma registrada na OFB.* *Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório ou* Definitivo*) pela data de início da execução da OFB.*	
Periodicidade	*Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.*	
	IAE = $\frac{TEX - TEST}{}$ *Onde:* ***IAE** – Indicador de Atraso de Entrega da OFB;*	

Mecanismo de Cálculo (métrica)	***TEX*** *– Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.* *A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.* *A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.* ***TEST*** *– Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.*
Observações	*Obs1: Serão utilizados dias corridos na medição.* *Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.*
Início de Vigência	*A partir da emissão da OFB.*
Faixas de ajuste no pagamento e Sanções	*Para valores do indicador* ***IAE****:* *Menor ou igual a 0 – Pagamento integral da OFB;* *De 1 a 60 - aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso.* *Acima de 60 - aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.*

IDA **– INDICADOR DE DISPONIBILIDADE DO AMBIENTE**	
Tópico	***Descrição***
Finalidade	Medir a disponibilidade da solução de conectividade sem fio do ponto de vista do usuário (em dias úteis).
Meta a cumprir	IDA ≥ 98%
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção.
Forma de acompanhamento	É apurado pelos fiscais técnicos do contrato.
Periodicidade	Mensal

Mecanismo de Cálculo (métrica)	IDA = 100 * (P1 / P2) Onde: IDA = Indicador de disponibilidade do ambiente. P1 = Soma da disponibilidade média (em minutos) dos componentes da solução no mês em análise e em dias úteis. P2 = Quantidade de dias úteis no mês em análise * 24 horas * 60 minutos
Observações	OBS1: Serão utilizados dias úteis na medição. OBS2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. OBS3: Os componentes da solução envolvem pontos de acesso, solução de gerenciamento e switches de acesso. OBS4: Mediante justificativa, poderão ser descontados do cálculo do indicador indisponibilidades causadas por fatores externos à solução (Ex: interrupção da energia elétrica ou manutenção programada).
Início de Vigência	*A partir da emissão da OFB.*
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IDA: • IDA ≥ 98%: sem descontos; • 95% IDA < 98%: desconto de 10% no valor da OS; • 90% IDA < 95%: desconto de 15% no valor da OS; • IDA < 90%: desconto de 20% no valor da OS + Advertência.

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

não produzir os resultados acordados;

deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

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

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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. Em caso de reincidência em até 3(três) vezes, 5% sobre o valor total do Contrato.
	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de	A sanção prevista no inciso III do **caput** do art. 156 da Lei nº 14.133/21 será aplicada ao responsável pelas infrações administrativas

2	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.	previstas nos incisos II, III, IV, V, VI e VII do **caput** do art. 155 desta Lei, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A CONTRATADA será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	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 5% sobre o valor total do Contrato. Em caso de reincidência po até 2 (duas) vezes, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	A CONTRATADA será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
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 de 48 horas úteis.	Multa de 5% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 02 (dois) dias úteis. Após o limite de 02 (dois) dias úteis, aplicar-se-á multa de 10% do valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de software (sistemas, portais, funcionalidades, banco de dados, programas,	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, em prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	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, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	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, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.

12	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, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
13	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10% do valor total do Contrato.

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

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

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

CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis após a verificação da qualidade e quantidade do material e a consequente aceitação mediante termo detalhado, a contar da comunicação formal por parte da CONTRATADA, informando que a solução está devidamente instalada, configurada e com o repasse de conhecimento realizado, incluindo na formalização a documentação exigida nos “requisitos de implantação” indicados neste Termo.

Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite mencionado no inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será reduzido pela metade.

O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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.

O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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.

Liquidação

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.

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.

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:

o prazo de validade;

a data da emissão;

os dados do contrato e do órgão Contratante;

o período respectivo de execução do contrato;

o valor a pagar; e

eventual destaque do valor de retenções tributárias cabíveis.

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;

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.

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).

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.

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.

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.

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

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.

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

Forma de pagamento

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

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

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

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

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

Antecipação de pagamento

Não será realizada antecipação de pagamento.

Cessão de crédito

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.

As cessões de crédito não fiduciárias dependerão de prévia aprovação do Contratante.

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

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, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

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 e Anexos)

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

8. Do reajuste

O objeto será contratado pelo preço ofertado na proposta da empresa vencedora juntada aos autos. O preço permanecerá e irreajustável pelo período de 12 (doze) meses, nos termos do § 3°, art. 135, da lei 14.133/2021, quando então se promoverá a sua correção de acordo com a variação do Índice de Custos de Tecnologia da Informação - ICTI, em conformidade com o art. 24 da Instrução Normativa nº 94/2022, tomando-se por base o índice vigente no mês de apresentação da proposta ou do orçamento a que essa se referir.

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

O preço ajustado também poderá sofrer correção desde que reste comprovada a ocorrência de quaisquer das hipóteses previstas na alínea “d”, do inciso II, do art. 124, da Lei nº 14.133/21.

9. Critérios de seleção do fornecedor

FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

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.

O regime de execução do contrato será o fornecimento e prestação de serviço associado: regime de contratação em que, além do fornecimento do objeto, o contratado responsabiliza-se por sua operação, manutenção ou ambas, por tempo determinado, de acordo com o art. 22, inciso V da Instrução Normativa SGD/ME nº 94, de 2022.

Da Aplicação da Margem de Preferência

Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

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

Habilitação jurídica

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;

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

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;

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;

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.

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

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.

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.

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

Habilitação fiscal, social e trabalhista

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

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.

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

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;

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

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

Caso o fornecedor seja considerado isento dos tributos 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.

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

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;

Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

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

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.

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.

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 patrimônio líquido mínimo de 5% do valor total estimado da contratação.

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).

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

Registro ou inscrição da empresa na entidade profissional em plena validade.

Comprovação de aptidão para o fornecimento de bens similares 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 emitidos pelo conselho profissional competente, quando for o caso.

Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

- Fornecimento de bens ou serviços de no mínimo 50% do item referente a hardwares.
- Será admitida, para fins de comprovação de quantidade mínima, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 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.

- Apresentar documentação técnica (manuais e/ou catálogos do fabricante, em mídia eletrônica ou URL) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto-a-ponto, com indicação de nome do documento e página que comprova o atendimento.

- Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante, somente documento oficial.

10. Estimativas do valor da contratação

Valor (R$): 7.877.601,58

A estimativa de custo total para a presente aquisição, de acordo com as necessidades do Ministério das Cidades, é de **R$ 7.877.601,58 (sete milhões, oitocentos e setenta e sete mil seiscentos e um reais e cinquenta e oito centavos)** conforme tabela detalhada abaixo:

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	TOTAL
1	Solução de segurança em Cluster para proteção avançada de perímetro - Firewall - denominada Next Generation Firewall (NGFW) com suporte, garantia e licenciamento inclusos para 60 meses com repasse de conhecimento.	Unidade	4	R$ 1.896.136,16	R$ 7.584.544,64
2	Solução para Gerenciamento de LOGS e Automação	Unidade	1	R$ 137.419,70	R$ 137.419,70
3	Solução para Gerenciamento Centralizado de NGFW	Unidade	1	R$ 88.123,00	R$ 88.123,00
4	Instalação e Configuração	Unidade	1	R$ 67.514,24	R$ 67.514,24
VALOR GLOBAL ESTIMADO				**R$ 7.877.601,58**	

11. Adequação orçamentária

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

A contratação do Ministério das Cidades será atendida pela seguinte dotação:

Gestão/Unidade: 0001/56101

Fonte de Recursos: 100

Programa de Trabalho: 56101.04.122.0032.2000.0001

Elemento de Despesa: 40

Plano Interno: INFORMÁTICA

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 do MCID

O Cronograma Físico-Financeiro representa o desenvolvimento previsto para a execução total do objeto desta contratação em relação ao tempo, observado o prazo de execução proposto, itens, etapas, fases, seus respectivos custos e pagamentos por parte da contratante.

O Cronograma Físico deverá, obrigatoriamente, ser compatível com o prazo de execução proposto pela contratante e com o orçamento apresentado, tanto no que se refere aos itens quanto aos valores do cronograma de desembolso.

Cronograma Físico Financeiro				
1 ano	**2 ano**	**3 ano**	**4 ano**	**5 ano**
2024	**2025**	**2026**	**2027**	**2028**
R$ 7.877.601,58	R$ -	R$ -	R$ -	R$ -

OBS: A depender do período da licitação o cronograma físico financeiro deverá ser ajustado.

12. Parcelamento da solução

Parcelamento da Solução de TIC

Os itens a serem licitados no lote 1 possuem complexidade tecnológica que exigem integral compatibilidade entre os equipamentos a serem adquiridos.

Contratar empresas distintas para o fornecimento e os serviços de instalação pode gerar conflito de responsabilidade entre as empresas envolvidas. Dessa forma, apesar de os serviços poderem ser mantidos por empresas diversas, por uma questão de ganho de escala e simplificação dos processos administrativos, a contratação de um único fornecedor é preferível.

Denota-se que o caso em comento apresentou todos os requisitos para agrupamento dos itens, tanto o requisito de viabilidade técnica quanto de viabilidade econômica, pois, houve respeito à integridade do objeto, atendendo a satisfação do interesse público, bem como trouxe benefícios para a Administração licitante.

Sabe-se, ainda, que é prática amplamente disseminada no mercado a produção pelos fabricantes de componentes e softwares de forma separada e somente para atender aos seus equipamentos, criando, nesse sentido, relação de exclusividade entre os equipamentos e seus softwares, o que determina condições de interoperabilidade.

O agrupamento dos itens em lote é, portanto, necessário ao perfeito provimento de equipamentos, softwares e componentes para pleno funcionamento da solução. Do contrário, haveria risco real da não interoperabilidade entre os equipamentos, componentes e softwares, decorrente das diferenças dos equipamentos de diversos fabricantes.

Além de garantir interoperabilidade, a licitação por lote proporcionará maior padronização dos equipamentos do parque tecnológico do MCID, o que trará impactos positivos no que tange à operação e manutenção dos equipamentos, uma vez que os produtos de mesma categoria ou função serão adquiridos de um mesmo fabricante.

A reunião dos itens em lote justifica-se, ainda, pela possibilidade de responsabilização de um único fornecedor no momento da integração e funcionamento da solução, uma vez que, na hipótese de uma contratação separada, poderia se tornar difícil a identificação do responsável pela ocorrência de uma eventual falha na solução adquirida, pois cada fornecedor poderia alegar que a falha decorre de equipamento, software, ou componente fornecido pelo outro.

A fim de obstar possíveis argumentos de transferência de responsabilidade, o MCID teria que se suprir com equipe técnica especializada capaz de fazer testes e identificar qual equipamento deu causa a cada ocorrência de falha, o que seria oneroso e demandaria nova contratação para a prestação de serviços terceirizados. Tal situação pode ser evitada com a reunião dos itens em lote, garantindo a contratação de um único fornecedor para prestar a solução e anulando possibilidades de transferência de responsabilidade entre fornecedores.

Ressalta-se, ainda, que esses riscos indesejáveis teriam que ser suportados, no mínimo, durante todo o período da garantia dos equipamentos, de 60 (sessenta) meses. A reunião em lote transforma a garantia de funcionamento dos equipamentos em garantia de funcionamento da “solução”, minimizando tais riscos.

13. Resultados e Benefícios

A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

Nesse sentido, o planejamento em tela almejou os seguintes resultados:

Eficiência com a redução do custo administrativo e operacional em função do agrupamento de itens em uma solução de segurança cibernética consolidada e unificada;

- Economia no valor da licitação em função do ganho de escala e na forma agrupada de contratação;
- Efetividade com a padronização dos itens previstos, subscrições e aumento da qualidade das especificações técnicas;
- Conformidade Legal: Adequação às legislações atuais, como a LGPD (Lei nº 13.709/2018) e o Marco Civil da Internet (Lei nº 12.965/2014).
- Segurança da Informação: Manutenção dos requisitos de segurança, garantindo a integridade, confidencialidade e disponibilidade dos dados.
- Visibilidade Aumentada: Melhoria na observação do uso de aplicações web e desktop, tráfego de rede e identificação de principais ameaças cibernéticas.
- Detecção em Tempo Real: Capacidade de detectar e prevenir ameaças cibernéticas imediatamente.
- Controle de Rede: Gestão do uso da rede, permitindo a aplicação de filtros e bloqueios de acordo com o perfil do usuário, controlando o acesso de maneira detalhada.
- Proteção do Ambiente: Defesa contra ameaças como worms, vírus, malwares e APTs, em conformidade com o Marco Civil da Internet.
- Geração de Relatórios: Produção de relatórios variados para uma análise rápida sobre tráfego, aplicações, ameaças e usuários.
- Prevenção de Vazamento de Dados: Proteção contra exfiltração de dados, em linha com a LGPD.
- Controle de Acesso Geográfico: Implementação de restrições de acesso baseadas em geolocalização para evitar acessos indesejados de localidades específicas.
- Maior Controle da Solução: Aumento do controle sobre a solução adotada.
- Manutenção Pós-Contrato: Garantia de que a solução continuará a proteger o ambiente corporativo, mesmo após o término do contrato, oferecendo pelo menos um nível básico de proteção.

Ademais, destaca-se que a presente contratação está devidamente alinhada às demandas e necessidades de negócio do Ministério, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, e os riscos envolvidos são administráveis.

14. PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVA

A possibilidade de participação ou não em licitações de empresas em consórcio fica ao juízo discricionário da Administração, conforme amplamente discutido na Jurisprudência, como, por exemplo, os Acórdãos nº 1.165/2012-Plenário, 1.946/2006-Plenário, 22/2003-Plenário, abaixo transcritos.

Assim, como é de amplo conhecimento daqueles que lidam com licitações, a jurisprudência desta Corte aponta para o caráter discricionário no que concerne à decisão acerca da participação de consórcios nos diversos eventos licitatórios, a teor do art. 33 da Lei de Licitações. Acórdão 1165/2012-Plenário.

Acórdão TCU nº 1.946/2006 – Plenário: a permissão da participação de consórcio é uma escolha discricionária do administrador, a ser analisada em cada caso concreto, dependendo do requisito de alta complexidade ou relevante vulto da obra, o qual não se acha presente na licitação do TST.

Acórdão nº 22/2003 – Plenário: No mesmo sentido é a regra insculpida no art. 33 da Lei nº 8.666/93, que estipula as normas a serem seguidas pela Administração nas hipóteses em que for permitida a participação de consórcios na licitação. Trata-se de escolha discricionária da Administração, a ser verificada caso a caso. Muitas vezes, a formação de consórcio pode ensejar redução no caráter competitivo, pois facilitaria que empresas, que seriam naturalmente competidoras entre si, acordassem para participar da licitação.

Considerando as características do objeto, não será admitida a participação de consórcios e cooperativas.

15. ALTERAÇÃO SUBJETIVA

É admissível a fusão, cisão ou incorporação da CONTRATADA com/por outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado; e haja a anuência expressa da Administração à continuidade do CONTRATO.

16. 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.

EMERSON MOREIRA DE MORAIS

Integrante Requisitante

Assinou eletronicamente em 06/01/2025 às 14:54:35.

ALINE BARROS DE SOUSA

Integrante Técnico

Assinou eletronicamente em 06/01/2025 às 12:20:47.

HAROLDO RODRIGUES DA SILVA

Integrante Administrativo

Assinou eletronicamente em 07/01/2025 às 10:40:41.

LUCAS MENDES DOS SANTOS

Autoridade Máxima da Área de TIC

Assinou eletronicamente em 06/01/2025 às 13:15:16.

RODRIGO DALVI SANTANA

Autoridade Competente

Assinou eletronicamente em 07/01/2025 às 18:06:00.