TERMO DE REFERÊNCIA

REGISTRO DE PREÇOS PARA PRESTAÇÃO DE SERVIÇOS DE EXPANSÃO DE SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO CHECKPOINT COM SOLUÇÃO DE BALANCEAMENTO DE FIREWALL CORPORATIVO E APPLIANCES FÍSICOS DO TIPO "NEXT GENERATION THREAT PREVENTION" E SUPORTE TÉCNICO.

Abril de 2022.

1. DO OBJETO

1.1. Registro de Preços para Prestação de Serviços de Expansão de Solução de Proteção de Perímetro Checkpoint com solução de Balanceamento de Firewall corporativo e Appliances físicos do tipo "Next Generation Threat Prevention", incluindo garantia, licenciamento e serviços de suporte técnico especializado por 24 (vinte e quatro) meses, conforme descritos, caracterizados e especificados neste Termo de Referência."

1.2. O objeto descrito neste Termo de Referência é caracterizado como comum, sendo cabível a utilização da modalidade de licitação denominada Pregão, tendo em vista que foi objetivamente definido neste documento por meio de especificações usuais do mercado.

1.3. Trata-se de objeto disponível em mercado próprio, fornecido habitualmente, independentemente da demanda da Administração, de forma padronizada, sem a exigência de atendimento de qualquer especificidade ou variantes de adequação.

2. DA DESCRIÇÃO DO (S) SERVIÇO(S), MATERIAL (IS)/EQUIPAMENTO (S)

Lote	Item	Descrição	Qtd
1	1	16600 HyperScale Appliance for Maestro including 2 100 GbE direct attach cables- Inventory Unit - CPAP-SG166XX-HS-MHS-INV	2
		SW 16600 HyperScale Appliance for Maestro including 2 100 GbE direct attach cables with SandBlast subscription package for 1 year	2
		Maestro Hyperscale Orchestrator 140 INV - CPAP-MHO-140-INV	2
		SW Maestro Hyperscale Orchestrator 140 with 8x 100 GbE and 48x 10 GbE ports	2
		100 GbE Direct Attach Cable (DAC), 3m - CPAC-DAC-100G-3M	2
		10Base-T Copper transceiver, compatible with CPAC-4-10F-C only - CPAC-TR-10T-C	8
		SFP transceiver for 1G fiber ports - short range (1000Base-SX) compatible with CPAC-4-1F-C only - CPAC-TR-1SX-C	10
		Serviços de instalação e configuração da solução	2
	2	Enterprise Software Subscription and Premium Support - CPES-SS-PREMIUM.1000	2
		Next Generation Threat Prevention and Sandblast for additional 1 year for 16600 HS Appliance - CPSB-SNBT-16600-HS-1Y	2
2		Serviços de suporte técnico especializado	24 meses

Tabela 1

2.1. ENTERPRISE FIREWALL COM BALANCEADOR DE CARGA

Os equipamentos deverão vir acompanhados dos conectores e cabeamentos necessários à sua implantação e pleno funcionamento;

2.1.1. Não serão aceitas soluções com software e hardware de fabricantes distintos, ou mesmo soluções de uso geral como, Servidores, Estações de Trabalho ou Equipamentos como Blades;

2.1.2. Não poderá ter seu fim de venda (End-of-Sale) e fim de vida (End-of-Life) anunciado no momento do aceite definitivo de sua entrega. Caso seja essa a situação, o fornecedor deverá entregar um modelo equivalente ou superior ao que entrou em Fim de Venda e/ou Fim de Vida;

2.1.3. Em caso de anúncio do EOS (Fim de Venda) e/ou EOL (Fim de Vida) ocorrer após o aceite definitivo da entrega da solução, o fim de suporte (End-of-Support) não poderá ocorrer nos próximos 60 (sessenta) meses a contar da emissão do Memorando de Início;

2.1.4. Os componentes da solução (hardwares e softwares) deverão ser fornecidos com todas as licenças necessárias ao seu pleno funcionamento de modo a realizar todas as funcionalidades descritas no Termo de Referência;

2.1.5. Os equipamentos deverão possuir 2 (duas) fontes de alimentação redundantes, do tipo hot-swappable, com alimentação de 100~120VAC e 210~240VAC e frequência de 50 ou 60 Hz ou auto-ranging. Os cabos de alimentação devem vir com, no mínimo, 1,80m e com plugue padrão ABNT NBR 14136 (três pinos);

2.1.6. Os equipamentos deverão possuir a altura máxima de 4 U (quatro rack units);

2.1.7. Os equipamentos deverão vir acompanhados de todos os acessórios que são necessários para sua fixação em rack bastidor padrão com largura de 19" (dezenove polegadas).

2.2. CARACTERÍSTICAS GERAIS DA SOLUÇÃO ENTERPRISE POR EQUIPAMNETO.

2.2.1. A solução deve possuir um throughput de tráfego real, por appliance, de no mínimo 17 Gbps (dezessete Gigabits por segundo) com todas as funcionalidades de proteção/inspeção descrita neste Termo de Referência ativadas simultaneamente.

2.2.2. Deve suportar, no mínimo, 32.000.000 (trinta e dois milhões) de conexões simultâneas para cada applicance.

2.2.3. Devem suportar 370.000 (trezentos e setenta mil) novas conexões por segundo para cada appliance;

2.2.4. Cada appliance deverá ser fornecido com a sua capacidade máxima de memória e de processamento.

2.3. DAS INTERFACES:

2.3.1. Cada appliance deve possuir a seguinte quantidade de interfaces:

2.3.1.1. 02 (duas) interfaces de 100Gb para comunicação com os balanceadores de carga;

2.3.1.2. Mínimo de 01 (uma) porta do tipo console para configuração e gerenciamento via linha de comando (CLI).

2.3.1.3. Cada equipamento deverá vir acompanhado do respectivo cabo para conexão via console;

2.3.1.4. Deve possuir, pelo menos, 01 (uma) interface de rede 1GBps (padrão 10/100Base-T e/ou 1000Base-X, com transceptor multimodo incluído) dedicada ao gerenciamento do Appliance;

2.3.1.5. Deve possuir interface dedicada para interconexão com outro equipamento de modo a compor um cluster de pelo menos 4 (quatro equipamentos);

2.3.1.6. Deve possuir, pelo menos, 01 (uma) interface para gerência out-of-band, que não dependa do sistema operacional regular do equipamento, fornecendo assim um acesso a console via rede.

2.3.1.7. Deve ser fornecido com todas as suas portas de comunicação, interfaces de redes e afins habilitadas, operacionais e prontas para operação, juntamente com seus respectivos transceptores, sem custos adicionais;

2.4. DAS FUNCIONALIDADES BÁSICAS DOS APPLIANCES NG FIREWALL.

2.4.1. Os Appliances devem permitir acesso ao equipamento via interface de linha de comando (CLI), console, SSH além de interface web HTTPS;

2.4.2. Devem ser capazes de criptografar e autenticar a comunicação com a solução de gerenciamento centralizado e/ou de orquestração;

2.4.3. Devem possuir número ilimitado de máquinas e usuários protegidos;

2.4.4. Devem implementar os protocolos IPV4 e IPV6;

2.4.5. Devem permitir a utilização simultânea de políticas de segurança tanto para IPV4 quanto para IPV6;

2.4.6. Devem suportar os protocolos DHCP e DHCPv6;

2.4.7. Devem implementar DHCP Relay;

2.4.8. Devem implementar agregação de link (link aggregation) via padrão 802.3ad e LACP;

2.4.9. Devem suportar o protocolo NTP;

2.4.10. Devem suportar os roteamentos estático para IPV4 e IPV6;

2.4.11. Devem suportar os seguintes protocolos de roteamento RIP, OSPF v2, OSPF V3 E BGP v4;

2.4.12. Devem suportar os protocolos H.323, SIP, SCCP e MGCP, de modo a dar suporte;

2.4.13. Devem suportar os protocolos RTCP, RTMP, RTSP e RTP;

2.4.14. Devem implementar o mínimo de 1024 (mil e vinte e quatro) VLANs ativas, no padrão 802.1q;

2.4.15. Devem suportar os protocolos SNMP v2 e SNMP V3;

2.4.16. A MIB SNMP deve contemplar, no mínimo, os seguintes indicadores: Consumo de CPU, Consumo de Memória, Temperatura, além de possuir indicadores de desempenho do equipamento.

2.4.17. Devem implementar Sflow e/ou NetFlow;

2.4.18. Devem implementar políticas de roteamento baseado em endereço IP de origem, endereço IP de destino e porta de comunicação;

2.4.19. Devem suportar o funcionamento no modo "sniffer", para inspeção de tráfego gerado por uma porta espelhada, para layer 2 e layer 3;

2.4.20. Devem possuir mecanismo de Backup/Restore de suas configurações e regras de segurança;

2.4.21. Devem possuir o agendamento automático de backups;

2.4.22. Devem armazenar os Backups internamente além de permitir, mesmo que através da gerência, que sejam transferidos para servidores externos;

2.4.23. Devem implementar regras de acesso por IPs de origem, IPs de destino, bem como agrupamentos de IPs de origem e/ou destino;

2.4.24. Devem implementar regras de acesso por sub-rede IP, tanto para origem quanto para destino;

2.4.25. Devem implementar regras de acesso a qualquer perímetro de segurança criada, relacionando-as a um usuário específico ou grupo de usuários do Active Directory/LDAP;

2.4.26. Devem implementar regras de acesso para qualquer perímetro, para máquinas do domínio;

2.4.27. Devem implementar regras de acesso à internet baseadas em domínio;

2.4.28. Devem implementar mecanismo de captura de pacotes;

2.4.29. Devem possuir mecanismo de "anti-spoof";

2.4.30. Os Appliances devem implementar alta disponibilidade podendo operar nos modos Ativo-Ativo e Ativo-Passivo com todo o licenciamento habilitado para tal e sem perda de conexões;

2.4.31. No modo de operação de cluster, deverão ser sincronizadas, no mínimo, seções, configurações como regras de firewall, NAT, QoS, objetos de rede, certificados, associações de segurança de VPNs, tabelas FIB, entre outras;

2.4.32. Devem permitir o monitoramento de falha de link na operação em cluster;

2.4.33. Devem implementar o funcionamento em modo transparente, tipo "bridge";

2.4.34. Devem permitir o sincronismo de configurações entre equipamentos do cluster de forma automática ou por console de gerência centralizado;

2.4.35. Devem implementar a tradução de endereços "NAT", nos seguintes modos: um-para-um, N-para-um, um-para-N e N-para-N;

2.4.36. Devem permitir que um endereço tenha mais de um NAT associado, em função da origem, destino ou porta;

2.4.37. Devem implementar NAT de origem e NAT de destino simultaneamente na mesma política;

2.4.38. Devem permitir o registro de eventos de NAT no LOG, com as informações de endereço interno, endereço público, data e hora do evento além de portas de origem e destino;

2.4.39. Devem possibilitar o registro em LOG de informações de cada sessão, de modo a armazenar endereços de IP de origem e destino, traduções de NAT, portas, protocolos, identificação de usuário e ação sobre o pacote (permitido ou negado);

2.4.40. Devem permitir a configuração e envio simultâneo de LOG para mais de um servidor de LOG;

2.4.41. Devem suportar o balanceamento de, no mínimo, 2 (dois) links distintos;

2.4.42. Devem ser capazes de bloquear sessões TCP que utilizarem variações do 3-way handshake, como 4-way e 5-way split handshake, de modo a prevenir possíveis tráfegos maliciosos;

2.4.43. Devem permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

2.4.44. Devem exibir nos logs do tráfego, o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver decripografia de SSL;

2.4.45. Devem permitir a consulta a fontes externas de domínios, URLs e endereços IP de modo a adicioná-los às políticas de firewall para bloqueio ou permissão;

2.4.46. Devem ser capazes de descriptografar, inspecionar e criptografar novamente o tráfego criptografado SSL, "inbound" e "outbound";

2.4.47. Devem permitir a criação de políticas de inspeção de tráfego para bloqueio dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg;

2.4.48. Devem suportar objetos IPV6 de modo a permitir a criação de regras com esses objetos;

2.4.49. Devem suportar agendamento de ativação de políticas, permitindo habilitar e desabilitar, automaticamente,

2.5. DAS CARACTERÍSTICAS DE QUALIDADE DE SERVIÇO.

2.5.1. Deve prover funcionalidades para controle e gerenciamento do tráfego ("Traffic Shaping"/ QoS - "Quality of Service") de entrada e saída (tráfego inbound e outbound) da rede ou zona de segurança;

2.5.2. Deve possibilitar a configuração de políticas de traffic shaping por tipo de aplicação, incluindo, entre outras, aplicações de áudio/vídeo (exemplo: Skype, Youtube), aplicações de compartilhamento de arquivos do tipo peer-to-peer, aplicações de redes sociais, aplicações de comunicação, aplicações de armazenamento em nuvem (exemplos: Dropbox, OneDrive, Google Drive);

2.5.3. Deve possibilitar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e SCCP;

2.6. DAS INSPEÇÕES DE TRÁFEGO CRIPTOGRAFADO.

2.6.1. Os Appliances devem ser capazes de inspecionar tráfego criptografado SSL, TLS1.3 e HTTP/2 "inbound" e "outbound";

2.6.2. Devem permitir a configuração de regras para inspeção SSL, por interface ou zona de segurança, baseadas no IP de origem e de destino, tipo de domínio, usuário/grupo de usuários do LDAP/Active Directory, URL e categoria;

2.6.3. Devem permitir a configuração de regras de exceção para que o tráfego SSL não seja inspecionado, por interface ou zona de segurança, baseadas no IP de origem e de destino, tipo de domínio, usuário/grupo de usuários do LDAP/Active Directory, URL e categoria;

2.7. DO CONTROLE DAS APLICAÇÕES.

2.7.1. O cluster de appliances deve implementar regras e políticas de segurança baseadas em aplicações, de modo a bloquear e/ou liberar aplicações (individuais ou em grupo) independentemente de porta ou protocolo que utilizem; 1.6.2 Deve implementar o controle para grupos estáticos e dinâmicos de aplicações, baseado em suas características e comportamentos;

2.7.2. Deve reconhecer no mínimo 3.300 (três mil e trezentas) aplicações diferentes, incluindo, entre outros, aplicações peer-to-peer, redes sociais, acesso remoto, protocolos de rede, update de software, voip, streeming de vídeo, áudio e vídeo, proxies, mensageiros instantâneos, compartilhamento de arquivos, email, etc.;

2.7.3. Deve reconhecer, no mínimo, as seguintes aplicações: http-proxy, http-tunnel, gnutella, youtube, facebook, facebook chat, twitter, linked-in, Skype, teamviewer, gmail, gmail chat, whatsapp, 4shared, onedrive, google drive, google docs, dropbox, db2, mysql, oracle, active directory, ldap, kerberos, radius, Citrix, ms-rdp, logmein, ftp, dhcp, itunes, dns, wins, msrpc, ntp, snmp, rpc over http webex, evernote, etc;

2.7.4. Deve ser capaz de visualizar e controlar as aplicações e os ataques que utilizam técnicas evasivas via comunicação criptografada, como Skype e ataques na porta 443;

2.7.5. Deve inspecionar o payload do pacote a fim de detectar assinaturas de aplicações conhecidas pelo fabricante independentemente de porta ou protocolo;

2.7.6. Deve ser capaz de determinar se uma aplicação está utilizando, ou não, a sua porta padrão;

2.7.7. Deve decriptografar o pacote SSL para possibilitar a leitura do payload, a fim de verificar as assinaturas de aplicações conhecidas pelo fabricante;

2.7.8. Deve permitir a utilização de quaisquer aplicativos a determinados grupos de usuários e negar a outros;

2.7.9. Deve permitir a utilização de aplicações em nuvem apenas no modo coorporativo e bloqueá-las ao serem utilizadas no modo pessoal, como por exemplo: Office 365, Skype, aplicativos do google, gmail, etc;

2.7.10. As atualizações da base de assinaturas de aplicações devem ser atualizadas automaticamente, a qual deve ficar registrada em LOG;

2.7.11. Deve ser capaz de reconhecer aplicações em IPV6;

2.7.12. Deve ser capaz de limitar a banda de download e upload usada por aplicações ("traffic shaping"), baseado no IP de origem, usuários e grupos de usuários do LDAP/Active Directory;

2.7.13. Deve suportar diversos métodos de identificação e classificação de aplicações como: Verificação de assinaturas, decodificação de protocolos e análise heurística;

2.7.14. Deve permitir a criação de assinaturas personalizadas sem intervenção do fabricante;

2.7.15. Deve implementar o controle sobre aplicações conhecidas e desconhecidas;

2.7.16. A solução deve permitir emitir alerta ao usuário quando a aplicação for bloqueada;

2.7.17. Deve permitir que o controle de portas seja aplicado a todas as aplicações;

2.7.18. Deve permitir a criação de grupos de aplicações personalizados a partir da base de aplicações existentes;

2.7.19. Deve implementar o controle de banda para aplicações, categorias e grupos de aplicações;

2.7.20. Deve implementar o bloqueio e desbloqueio de aplicativos, sites e categorias em faixas de tempo pré-determinadas;

2.7.21. A solução deve permitir a criação de usuários administrativos específicos para funcionalidades de controle de acesso a aplicações;

2.7.22. Para cada regra de controle de acesso às aplicações, a solução deve ser capaz de desabilitar o registro de log, habilitar o registro de log e registrar a quantidade de tráfego enviado, recebido e o tempo de navegação.

2.8. DAS FUNÇÕES DE PREVENÇÃO DE INTRUSÃO

2.8.1. Os appliances que compõem a solução devem possuir funcionalidades de IPS (Intrusion Prevent System) integrado;

2.8.2. Devem possuir base de assinaturas de IPS com, no mínimo, 10.000 (dez mil) ataques conhecidos;

2.8.3. A solução deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente dos seus tamanhos;

2.8.4. Devem implementar a inspeção pelos mecanismos de análise de padrões de estado de conexões, de análise de decodificação de protocolo, de análise e detecção de anomalias de protocolo e de "IP fragmentation";

2.8.5. Devem suportar análise e decodificação dos protocolos de rede de camada 2 até camada 7 do modelo OSI (Open System Interconnection);

2.8.6. Devem ser capazes de decodificar e analisar, no mínimo, 120 (cento e vinte) protocolos, entre os quais deverão constar: DHCP, DHCP versão 6, DNS, HTTP, HTTPS, FTP, FINGER, ICMP versão 4, ICMP versão 6, IMAP, H323, SIP, SCCP,
MGCP, IP versão 4, IP versão 6, LDAP, NetBIOS, POP3, NFS, NTP, RADIUS, SNMP, SMTP, SSH, SSL, TLS, RPC, TELNET, TCP, UDP, FTP e TFTP;

2.8.7. A solução deve reconhecer pelo menos os seguintes protocolos: Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IPv4 encapsulation, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC UA Binary, OPC UA, Oracle, MySQL, POP3, POP3S, SIP, SRP, SSH, TELNET, WINS, X11, RTSP, SMTP, SunRPC, NNTP, SCCP, SMB, SMB2, TFTP e demais protocolos constantes do item 1.3 e seus subitens;

2.8.8. Devem ser capazes de identificar ataques para todos os protocolos de rede independentemente das portas a que estejam relacionados para no mínimo os seguintes protocolos: FTP, HTTP, HTTPS, POP3, SMTP, IMAP, DNS, SNMP e RPC; 1.7.9 Devem ser capazes de realizar análise e inspeção Statfull (mantendo-se o estado da conexão) e análise e inspeção Stateless;

2.8.9. Devem suportar análise de tráfego na direção servidor-cliente, ou seja, ataques originados no ambiente externo e direcionados a usuários internos (Client-side Attacks ou Drive-by Attacks);

2.8.10. Devem ser capazes de detectar bloqueio de ataques direcionados a servidores de aplicação Web (Web Application), através de tecnologia heurística ou assinaturas próprias para a proteção contra este tipo de ataque em, no mínimo, sql-injection e buffer overflow;

2.8.11. Devem ser capazes de obter informações detalhadas sobre ataques para localização geográfica, reputação de aplicação e reputação de protocolo;

2.8.12. Devem implementar algoritmo de pontuação para a relevância de um ataque conforme padrão de mercado e definido por entidade independente (Common Platform Enumeration), CVE ID ou Bugtraq ID, ou suportar mecanismo próprio de pontuação de ataques, permitindo distinguir quando um ataque for permitido ou bloqueado;

2.8.13. A solução deve suportar a análise do nível de relevância de um ataque, permitindo uma demonstração de faixa de relevância para, no mínimo, 4 (quatro) níveis;

2.8.14. Devem suportar as categorias de ataques e tipos de ameaças, conforme padrões de mercado e definidos por entidades independentes, podendo estas serem importadas em padrão Snort;

2.8.15. Devem suportar a configuração e administração para, no mínimo, os seguintes itens:

2.8.15.1. Perfis de DoS (Denial-of-Service) e DDoS (Distributed Denial-of-Service);

2.8.15.2. Regras de ACL (Access Control List);

2.8.15.3. Contextos de administração (Virtual IPS) que devem ser configurados por VLAN (IEEE 802.1Q) e CIDR (Classless Inter-Domain Routing);

2.8.16. Devem ser capazes de detectar e bloquear ataques do tipo Denial-of-Service (DoS) e Distributed Denial-of-Service (DDos) de forma nativa para:

2.8.16.1. Detecção e bloqueio efetivo baseado em assinaturas de ataques às vulnerabilidades de DoS, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures);

2.8.16.2. Detecção e bloqueio efetivo baseado em assinaturas de atividades de agentes (zumbis) DDoS, conforme padrões de mercado e definidos por entidades independentes (Computer Emergency Response Team e Common Vulnerability and Exposures);

2.8.16.3. Detecção e bloqueio de ataque SYN, que permita limitar e controlar a quantidade de requisições de conexões;

2.8.17. Devem ser capazes de identificar e bloquear ataques de Brute Force;

2.8.18. Devem implementar a Detecção e bloqueio baseados em políticas, para no mínimo:

2.8.18.1. Filtros de origem e destino por: país, nome (DNS), endereço IP, porta, bloco de endereços, rede ou grupo de redes;

2.8.18.2. VLAN ID para, no mínimo, 1024 VLANs;

2.8.18.3. Filtros de controle de aplicação: aplicação, grupo de aplicações, porta de comunicação customizada, serviço ou grupo de serviços;

2.8.19. Filtro de resposta com, no mínimo os itens seguintes:

2.8.19.1. Bloqueio (Drop);

2.8.19.2. Negação (Deny);

2.8.19.3. Quarentena (Bloquear ou negar um IP por tempo determinado após atingir a quantidade de eventos relativos a uma regra);

2.8.19.4. Ignorar.

2.8.20. Devem ser capazes de detectar e bloquear o tráfego de aplicações Instant Messenger, P2P (peer-to-peer) além de Proxies Anônimos;

2.8.21. Devem suportar a detecção e bloqueio de ataques através de tuneis para IPv4-in-IPv4, IPv4-in-IPv6 e IPv6-in-IPv6;

2.8.22. Devem suportar a detecção e bloqueio de ataques através de VLANs;

2.8.23. A solução deve ser capaz de não interromper ou alterar segmentos monitorados com protocolos de roteamento e redundância de rotas, ainda que trafegados dentro do protocolo LACP (Link Aggregation Control Protocol);

2.8.24. Devem permitir a criação de novas assinaturas de ataques;

2.8.25. Devem permitir a configuração e administração de ACL em camada 3 com as seguintes regras:

2.8.25.1. Permitir: O tráfego é enviado Inline sem inspeção completa dos pacotes;

2.8.25.2. Permitir e Prevenir Ataques: O tráfego é enviado Inline para inspeção completa dos pacotes;

2.8.25.3. Descartar: O tráfego será descartado;

2.8.26. Devem suportar a detecção de bloqueio de ataques, pelo menos, nas seguintes modalidades:

2.8.26.1. Inspeção de tráfego Statefull: IP defragmentation e TCP stream reassembly;

2.8.26.2. Por assinaturas: Definidas pelo fabricante e definidas pelo usuário;

2.8.26.3. Anomalias;

2.8.26.4. Por protocolos de camada 7 do modelo OSI;

2.8.27. Devem possuir detecção e bloqueio de ataques, independente de sistema operacional alvo;

2.8.28. Devem suportar a detecção heurística e consulta de reputação de atividades de agentes (zumbis) internos que pertençam a uma Botnet;

2.8.29. Devem implementar o bloqueio de tráfego inbound e outbound baseado em, no mínimo, protocolo, porta e serviço;

2.8.30. Devem implementar proteção contra downloads automáticos de arquivos executáveis maliciosos através do protocolo HTTP;

2.8.31. Devem implementar criação de políticas para bloqueio de download de arquivos por extensão e tipos de arquivo;

2.8.32. A solução deve suportar, no mínimo as seguintes categorias e tipos de ataques:

2.8.32.1. Reconnaissance: Brute force, Host Sweep, OS Fingerprinting e Port Scan;

2.8.32.2. Exploits: Arbitrary Command Execution, Backdoor, Bot, Buffer Overflow, Denial of Service, DDoS Agent Activity, Code/Script Execution, Evasion Atempt, Privileged Access, Probe, remote Access, Trojan, Virus e Worms;

2.8.32.3. Volume DoS: Statistical Deviation e Over Threshold ou possuir mecanismo que permita detecção e contenção de ataques DoS;

2.8.32.4. Policy Violations: Audit, Command Shell, Covert Channel e Non-standard Port;

2.8.33. Suportar assinaturas para detecção e bloqueio de ataques através de vulnerabilidades DoS e DDoS;

2.8.34. Devem suportar assinaturas para detecção e bloqueio de atividades de agentes (zumbis) DDoS;

2.8.35. Devem suportar aplicação e remoção de quarentena:

2.8.35.1. Sob demanda do administrador, o qual deverá ter a opção de inserir e remover um endereço IP da quarentena através de interface administrativa sem a necessidade de reinicialização do equipamento ou reaplicação de política;

2.8.35.2. Por períodos programáveis pelo administrador, podendo ser esses (os períodos) diferentes em cada regra;

2.8.35.3. Por remoção explicita, após expiração de tempo pré-determinado.

2.8.36. A solução deve suportar ajuste de bloqueio inteligente, baseado em assinaturas recomendadas pelo fabricante para bloqueio;

2.8.37. Deverá permitir a visualização de bloqueios de pacotes e de conexões, independente do motivo pelos quais ocorreram.

2.9. DAS DETECÇÕES DE AMEAÇAS (MALWARES, WORMS E SPYWARE).

2.9.1. A Solução deve realizar a detecção e bloqueio de códigos maliciosos, ameaças malwares e malwares avançados, vírus, worms e spyware em tempo real, utilizando-se os seguintes mecanismos:

2.9.1.1. Mecanismo de lista local de arquivos confiáveis (lista branca), os quais não precisarão ser analisados por serem confiáveis;

2.9.1.2. Mecanismo de lista com valores Hash de arquivos que sejam códigos maliciosos e ameaças (malwares) conhecidas e armazenado em uma base de dados local (lista negra);

2.9.1.3. Mecanismos de detecção de códigos maliciosos e ameaças (malwares), que deve operar em tempo real, para no mínimo, arquivos PDF, objetos e arquivos Flash, arquivos executáveis, arquivos Microsoft Office, HTML, JavaScript, arquivos comprimidos (exemplo: zip, gzip, etc).

2.10. DA SOLUÇÃO DE ANTIBOT.

2.10.1. A solução prover proteção contra tráfego de "botnets" (identificar e bloquear comunicação com redes "botnet"); 1.9.2 Deve possuir mecanismos de detecção variados e que incluam pelo menos: verificação de endereço IP e descrição da comunicação;

2.11. DA RESPOSTA AOS ATAQUES.

2.11.1. Deve implementar as seguintes ações de resposta: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar "tcp-reset";

2.11.2. Deve implementar a atualização global de bloqueio para determinado ataque de modo a propagar e atualizar todas as políticas;

2.11.3. Deve suportar a captura de pacotes para análise de evidências em formato LIBPCAP (Library for Packet Capture);

2.11.4. Deve suportar o envio de Trap SNMP para SNMPv2 e SNMPv3;

2.11.5. Deve implementar o envio de e-mail;

2.12. DAS FUNCIONALIDADES DE VPN (VIRTUAL PRIVATE NETWORK).

2.12.1. A solução de appliances devem possuir funcionalidades de concentrador VPN conforme se segue;

2.12.2. Deve implementar VPN IPSEC;

2.12.3. A VPN IPSEC deve ser implementada nas modalidades "site-to-site" e "cliente-to-site";

2.12.4. Deve implementar VPN SSL;

2.12.5. Deve implementar VPNs SSL utilizando certificados digitais;

2.12.6. A solução deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos Tuneis VPN SSL;

2.12.7. A VPN IPSEC deve ser implementada com as seguintes funcionalidades/algoritmos:

2.12.7.1. Suporte aos algoritmos de criptografia DES, 3DES, AES-128 e AES-256;

2.12.7.2. Suporte à autenticação MD5 e SHA-1;

2.12.7.3. Suporte a "Diffie-Hellman" Group 1, Grtoup 2, Group 5 e Group 14;

2.12.7.4. Suporte ao algoritmo "Internet Key Exchange" - IKE v1 e v2;

2.12.7.5. Suporte a autenticação via certificado IKE PKI;

2.12.8. Deve permitir a interoperabilidade de VPN site-to-site com, no mínimo, os seguintes fabricantes: Checkpoint, Cisco, Fortinet, Junjiper, Palo Alto, Sophos e Sonic Wall;

2.12.9. A VPN IPSEC deve ser implementada por meio de conexão via Web bem como por meio de conexão via cliente VPN instalado no computador do usuário;

2.12.10. A VPN SSL deve possibilitar o acesso à rede interna e/ou zona de segurança do contratante, de acordo com a política de segurança para esta finalidade;

2.12.11. A VPN SSL deve suportar autenticação via LDAP/Active Directory, certificado digital e também na base de usuários local;

2.12.12. A VPN SSL deve implementar o controle de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário/grupo de usuários do LDAP/Active Directory;

2.12.13. A VPN SSL deve permitir a atribuição de endereço IP dinâmico aos usuários remotos, de modo a permitir a configuração e utilização de faixa de endereços IP específica ou range de IPs específicos para clientes VPN;

2.12.14. A VPN SSL deve permitir a atribuição de endereço IP fixos aos clientes remotos;

2.12.15. A VPN SSL deve possibilitar configuração que direcione todo o tráfego dos usuários remotos de VPN para dentro do túnel de VPN, ou apenas o tráfego referente às rotas que o cliente recebe ao estabelecer a conexão VPN;

2.12.16. A VPN SSL deve possibilitar atribuição de DNS aos usuários remotos de VPN;

2.12.17. A solução de VPN SSL deve permitir a criação das seguintes de políticas de segurança para o tráfego dos seus usuários remotos: inspeção de tráfego SSL, controle de aplicações, IPS, antivírus, antispyware e filtro Web;

2.12.18. A VPN SSL deve permitir que seja identificado o sistema operacional (bem como a sua versão) utilizado pelo usuário;

2.12.19. A solução de VPN SSL deve possuir cliente VPN, próprio ou de terceiros, para, no mínimo, os sistemas operacionais Windows 7, Windows 8, Windows 10, Mac OS X, Apple IOS, Google Android e Linux;

2.12.20. A solução de VPN SSL deve possuir cliente, próprio ou de terceiros, para instalação em dispositivos móveis (sistemas operacionais Apple iOS e Google Android), em desktops (sistemas operacionais Windows e MAC OS X), e suportar conexões VPN "clientless" (VPN via browser) desses sistemas operacionais e também de Linux e Chrome OS;

2.12.21. A solução deve implementar NAT-T (NAT Transversal);

2.12.22. A VPN deve suportar e estar licenciada para, no mínimo:

2.12.22.1. Não limitar clientes de VPN SSL simultâneos;

2.12.22.2. Não limitar túneis de VPN IPSEC simultâneos;

2.12.22.3. Não limitar usuários simultâneos via conexão VPN "clientless" (VPN via browser);

2.12.22.4. Não limitar usuários simultâneos com conexões via cliente VPN e VNP site-to-site;

2.12.22.5. A solução deve permitir a arquitetura de VPN HUB e SPOKE.

2.13. DA PREVENÇÃO CONTRA AMEAÇAS DO TIPO ZERO-DAY E AMEAÇAS NOVAS.

2.13.1. A solução dever prover proteção contra malwares não conhecidos ("zero-day" /sem assinatura registrada);

2.13.2. A análise de malwares modernos em sandbox deverá ser realizada de forma interna no appliance do próprio fabricante ou em nuvem (serviço acessado pela Internet) do próprio fabricante;

2.13.3. A solução deverá prover proteção contra malwares não conhecidos (zero-day) nos tráfegos de entrada e saída com filtro de ameaças avançadas e análise de execução em tempo real; e inspeção de tráfego de saída de callbacks;

2.13.4. A solução deverá prover inspeção, bloqueio e alerta de tráfego de saída do tipo "callbacks" (comunicação do malware com o servidor de comando e controle);

2.13.5. A solução deve ser capaz de enviar arquivos trafegados de forma automática para análise "in cloud" ou localmente, onde o arquivo será executado e simulado em ambiente controlado (sandbox);

2.13.6. Deve permitir selecionar de forma granular quais tipos de arquivos serão inspecionados;

2.13.7. Deve prover a análise de arquivos maliciosos em sandbox, no mínimo, no sistema operacional Microsoft-Windows XP, Microsoft Windows 7 e Microsoft Windows 10;

2.13.8. Caso sejam necessárias licenças de sistemas operacionais e softwares para execução de arquivos na sandbox, as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

2.13.9. Deve permitir selecionar através de regras granulares quais tipos de arquivos serão inspecionados incluindo, no mínimo, endereço IP de origem/destino, usuário/grupo do Active Directory/LDAP, porta, tipo de arquivo bem como compor esses critérios na mesma regra;

2.13.10. Deve possuir a capacidade de diferenciar os arquivos inspecionados com pelo menos três níveis de intensidade da ameaça;

2.13.11. Deve implementar análise em sandbox, detecção e bloqueio de malwares nos seguintes tipos de arquivos:

2.13.11.1. Trafegados na Internet (downloads e anexos de e-mail) por meio dos protocolos HTTPS, HTTP e SMTP;

2.13.11.2. Executáveis, DLLs, ZIP e criptografados em SSL;

2.13.11.3. Do pacote MS-Office (exemplo: .doc, .docx, .xls, .xlsx, .ppt, .pptx, etc.);

2.13.11.4. Java (.jar e class);

2.13.11.5. Compactados (RAR, ZIP, 7-ZIP);

2.13.11.6. no formato PDF;

2.13.12. Deve possuir a capacidade de analisar em sandbox links (http e https) presentes no corpo de e-mails trafegados em SMTP. Caso a análise do link pela funcionalidade de sandbox o identifique como ameaça ou como site hospedeiro de exploits, deve ser gerado alerta/relatório e registrado em LOG;

2.13.13. A funcionalidade de análise de links deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

2.13.14. Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação do usuário vítima do ataque;

2.13.15. A solução deve possibilitar a criação de novas assinaturas e atualização automática da sua base de assinaturas para bloqueio dos malwares identificados em sandbox;

2.13.16. Deve permitir a criação de regras de exceção por Interfaces, zonas de segurança, sub-rede, endereço IP de destino ou origem, para que o tráfego não passe por esse tipo de inspeção;

2.13.17. A solução deve permitir visualizar a quantidade de arquivos enviados para análise em sandbox;

2.13.18. A solução deve prover mecanismo do tipo "painel de controle" e relatório onde seja possível a visualização de, no mínimo, as informações de sumário de detecção e proteção além de gráfico com as principais ameaças detectadas;

2.13.19. A solução deve prover relatório das análises em sandbox contendo detalhamento dos arquivos analisados (nome, extensão, tamanho, etc.), bem como detalhamento das atividades identificadas na análise, como alterações em arquivos do sistema operacional, alterações nos registros, utilização da rede, manipulação de processos, etc.;

2.13.20. Com base nos resultados das análises em sandbox a solução deve gerar assinaturas de antivírus e antispyware automaticamente e integrá-las à sua base de assinaturas contra ameaças;

2.13.21. Com base nos resultados das análises em sandbox a solução deve prover informações, no mínimo o seu endereço IP, sobre o usuário infectado;

2.13.22. A solução deve permitir exportar o resultado das análises de malwares "zeroday" em PDF.

2.14. DAS FUNCIONALIDADES DE FILTRO DE URL.

2.14.1. A solução deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs;

2.14.2. A solução deve permitir a criação de regras que possibilitem a permissão e bloqueio de acessos baseado no mínimo nos seguintes critérios:

2.14.2.1. Origem: grupos de domínio, serviços de diretório LDAP ou Active Directory e Aplicação;

2.14.2.2. Destino: categoria, domínio e url/lista;

2.14.2.3. Tipo de arquivo;

2.14.2.4. Horário, e período (dia, mês, ano, dia da semana) de modo a definir os períodos de funcionamento por regra;1.13.3 A solução deve permitir a definição de largura e percentual de banda máxima para o acesso, de acordo com o estabelecido em regra, baseando-se em IP de origem, grupos de usuários, categoria do destino e/ou protocolo; 1.13.4 A solução deve ser capaz de atuar como "man in the middle" de modo a intermediar e repassar todas as requisições;

2.14.2.5. Protocolos HTTP, FTP, entre outros;

2.14.2.6. A solução deve suportar certificados on-box, de modo a importar certificados válidos ou gerar certificados auto-assinados;

2.14.3. Deve permitir a emissão de páginas customizáveis de erro também aos sites criptografados;

2.14.4. Deve permitir controle de acesso através do percentual de largura de banda disponível para determinadas categorias e, os limites de banda devem der definidos por:

2.14.4.1. Limite geral ou percentual de banda, de modo a definir um limite para todos os usuários e aplicações na rede, de modo a restringir a quantidade de tráfego gerado;

2.14.4.2. Limite de banda por usuário, de modo a definir um limite para um usuário específico ou uma categoria de usuários.

2.14.5. A Solução deve permitir a definição de quota de acesso, de modo que determinados destinos (categorias, URLs, domínios ou listas) possam ser acessados por um período limitado de tempo;

2.14.6. Deve possuir mecanismo de classificação em tempo real dos sites visitados ou sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino;

2.14.7. Deve permitir o armazenamento em cache, a fim de melhorar a desempenho do acesso à internet.

2.14.8. A rede de reputação a que se refere o item anterior não deve somente ser baseada em informações de fluxo da própria base de appliances instalados, mas sim em correlações entre outros parâmetros: Listas negras de URL, listas Brancas de URL, listas de equipamentos comprometidos, volume global de tráfego, histórico dos sites, dados de categorização de URLs e web crawlers;

2.14.9. A solução deve permitir atualização automática da lista de URLs categorizadas via internet por meio de base proprietária do fabricante do equipamento;

2.14.10. Deve possuir mecanismo segurança que analise em tempo real a presença de conteúdo malicioso nas páginas acessadas;

2.14.11. Deve possuir mecanismo que gere alertas via e-mail quando há uma tentativa excessiva a um site bloqueado. Este alerta será disparado quando atingido o número de tentativas bloqueadas previamente pelo administrador para cada categoria;

2.14.12. Deve suportar o registro nos LOGs de informações das atividades dos usuários;

2.14.13. Deve suportar o registro/contabilização das atividades dos usuários que acessam a Internet. A solução deve possibilitar a geração de relatório gerencial por usuário contendo essas informações (URLs e aplicações acessadas, tempo utilizado no acesso por URL/aplicação);

2.14.14. Deve suportar métodos de manipulação de sites dinâmicos e sites web 2.0, ou seja, alterar seu comportamento de acordo com o conteúdo específico divulgado pelo site;

2.15. DAS FUNCIONALIDADES DE DLP (DATA LOSS PREVENTION).

2.15.1. A solução deve prover funcionalidades para proteção contra perda e vazamento de informações sensíveis à organização, de modo a impedir a saída de arquivos e informações da rede interna, o qual deverá funcionar para redes ou zonas de segurança;

2.15.2. Deve permitir a criação de regras com filtros que identifiquem e bloqueiem a transferência de arquivos pelo seu tipo, incluindo, mas arquivos do MS-Office, PDF entre outros;

2.15.3. As regras de que trata o item anterior devem ser capazes de inspecionar os seguintes tipos de aplicação: instant messaging, SMB, entre outras;

2.15.4. As regras de que trata o item 1.14.2 devem ser capazes de inspecionar os seguintes tipos de protocolo: HTTP, SMTP e FTP;

2.15.5. As regras de que trata o item 1.14.2 devem ser capazes de inspecionar tráfego HTTPS;

2.15.6. A solução deve permitir a identificação e o bloqueio de informações sensíveis como número de cartão de crédito;

2.15.7. A solução deve permitir a criação de novos tipos de dados para monitoramento e eventual bloqueio da transferência;

2.15.8. Deve suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses arquivos;

2.15.9. Deve possibilitar a criação de políticas de DLP por usuário/grupos de usuários do LDAP/Active Directory;

2.15.10. A solução deve prover interface para visualização do número de incidentes de DLP ou Filtro de Dados;

2.15.11. Será permitido que a funcionalidade de Data Loss Prevention seja fornecida em appliance separado.

2.16. DO BALANCEAMENTO DE CARGA PARA ENTERPRISE FIREWALL

2.16.1. Deverão ser fornecidos 2 (dois) equipamentos para assegurar continuidade do ambiente em caso de falha.

2.16.2. Deverá vir acompanhada dos conectores e cabeamentos necessários à sua implantação e pleno funcionamento;

2.16.3. Não serão aceitas soluções com software e hardware de fabricantes distintos, ou mesmo soluções de uso geral como, Servidores, Estações de Trabalho ou Equipamentos como Blades;

2.16.4. Não poderá ter seu fim de venda (End-of-Sale) e fim de vida (End-of-Life) anunciado no momento do aceite definitivo de sua entrega. Caso seja essa a situação, o fornecedor deverá entregar um modelo equivalente ou superior ao que entrou em Fim de Venda e/ou Fim de Vida.

2.16.5. Em caso de anúncio do Fim de Venda e/ou Fim de Vida ocorrer após o aceite definitivo da entrega da solução, o fim de suporte (End-of-Support) não poderá ocorrer nos próximos 60 (sessenta) meses a contar da emissão do Memorando de Início.

2.16.6. Os componentes da solução (hardwares e softwares) deverão ser fornecidos com todas as licenças necessárias ao seu pleno funcionamento de modo a realizar todas as funcionalidades descritas no Termo de Referência.

2.16.7. Deverá possuir 2 (duas) fontes de alimentação independentes, do tipo hot-swappable, com alimentação de 100~120VAC e 210~240VAC e frequência de 50 ou 60 Hz ou auto-ranging. Os cabos de alimentação devem vir com, no mínimo, 1,80m e com plugue padrão ABNT NBR 14136 (três pinos);

2.16.8. Deverá possuir a altura máxima de 4 U (quatro rack units);

2.16.9. Deverá vir acompanhados de todos os acessórios que são necessários para sua fixação em rack bastidor padrão com largura de 19" (dezenove polegadas).

2.16.10. A solução a que se refere este item terá por finalidade prover o balanceamento entre os appliances de Next generation Firewall, de modo a permitir que seus throughputs, suas capacidades de análise, capacidades de inspeção bem como todas as funcionalidades pedidas no item 1.2 e seus subitens sejam somados;

2.16.11. A solução de balanceamento deve permitir que a solução de NG Firewall se torne escalável;

2.16.12. A solução deve suportar a orquestração entre appliances de modelos diferentes, do mesmo fabricante, de modo a prover a escalabilidade ao longo do tempo.

2.16.13. A solução de balanceamento deverá ser fornecida em appliances físicos;

2.16.14. Os appliances deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações do Termo de Referência.

2.16.15. A solução deverá ser provida de forma redundante, de modo que se houver a falha de uma delas, a outra possa assumir totalmente o controle, sem que haja perda do tráfego;

2.16.16. A solução deve ser capaz de organizar os appliances de NG Firewall em grupos de segurança, nos quais os appliances de NG Firewall atuarão com seus recursos somados;

2.16.17. Cada Grupo de Segurança deverá comportar, no mínimo, 8 (oito) appliances;

2.16.18. A solução deverá ser capaz de suportar, no mínimo, 4 (quatro) grupos de segurança;

2.16.19. A solução deverá ser capaz de conectar, no mínimo, 24 (vinte e quatro) appliances Next Generarion Firewall a 10 Gbps com interfaces 10GBase-SR do tipo SFP+ e 4 Appliances a 100 Gbps de forma redundante.

2.16.20. A solução deverá possuir no mínimo 04 (quatro) interfaces de rede 10GBase-SR do tipo SFP;

2.16.21. A solução de balanceamento deverá ser conectada aos Appliances NGFirewall através de interfaces 100GB para cada gateway de forma redundante;

2.16.22. A solução deverá possuir a quantidade de transceptores suficientes para conectar toda a solução à rede corporativa, o que inclui a gerência.

2.16.23. A solução deverá ser capaz de processar internamente até 1Tbps.

2.17. DO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

2.17.1. O serviço especializado de instalação, configuração e migração entre as soluções deverão ser prestados por profissional certificado pelo fabricante da solução a ser disponibilizado à época da assinatura do contrato.

2.17.2. Compreende a instalação e customização dos equipamentos, montagem física dos equipamentos, e todos os componentes, bem como a configuração lógica de todos os equipamentos e softwares envolvidos na solução ofertada, de acordo com a topologia definida pela CONTRATANTE.

2.17.3. A CONTRATADA deverá apresentar sua equipe de trabalho, composta pelo Gerente de Projeto e sua equipe técnica, conforme o serviço a ser executado, na data da 1ª reunião de acompanhamento da execução do Contrato, a ser definida pelo CONTRATANTE, após a assinatura do mesmo.

2.17.4. Deverá ser apresentado plano de ação das atividades e cronograma de implantação, em até 15 dias úteis, contados da assinatura do contrato, incluindo as etapas de Kick-off, levantamento, topologia, montagem dos equipamentos, instalação, configuração, migração, testes e operação assistida da solução ofertada.

2.17.5. Cabe à CONTRATANTE, definir a topologia a ser implementada, e sua interligação aos demais equipamentos de rede existentes.

2.17.6. A equipe da CONTRATADA que irá executar a instalação deverá trabalhar sob a orientação e supervisão direta do profissional responsável (gerente de projeto) pela coordenação das atividades de implantação e migração e com o acompanhamento do profissional técnico indicado pelo CONTRATANTE. Caberá ao gerente de projeto coordenar e orientar todo o processo de planejamento, instalação, configuração, integração, migração e teste da solução, acompanhando o cumprimento dos prazos e atestando a qualidade dos entregáveis.

2.17.7. Deverá disponibilizar, no momento da assinatura do contrato, técnico especializado na solução ofertada pelo período necessário para realizar a instalação, configuração, parametrização, otimização para pleno funcionamento da solução.

2.17.8. Deverá instalar configurar e otimizar a solução ofertada com todos os componentes da solução em pleno funcionamento.

2.17.9. Deverá haver repasse de conhecimento de toda a solução implementada para a equipe designada como responsável técnica, com apresentações sobre a solução ofertada em local definido pela CONTRATANTE.

2.17.10. A janela de instalação, configuração, manutenção, será acordada com a CONTRATANTE, que poderá optar em ser executadas em finais de semana, feriados e fora do expediente, e em horário noturno, para evitar indisponibilidade.

2.17.11. Os eventuais custeios com deslocamentos técnicos, despesas de transportes, diárias, seguro ou quaisquer custos envolvidos ficam a cargo da CONTRATADA.

2.17.12. A CONTRATADA deve emitir relatórios das atividades da implementação e migração, deverão ser apresentados em via impressa e em meio digital, serão considerados como efetivamente entregues e aceitos somente após a validação pela equipe técnica da CONTRATANTE.

2.18. DO SUPORTE TÉCNICO ESPECIALIZADO

2.18.1. Prestar suporte especializado na solução contratada para garantir a manutenção emergencial, preventiva, corretiva, melhoria contínua e realizar as atualizações das licenças e assinaturas da solução;

2.18.2. Disponibilizar técnico especializado na solução ofertada no regime de 24 horas por 7 dia, durante o período de vigência do contrato, para garantir o perfeito funcionamento da solução;

2.18.3. Os serviços contratados poderão ser executados após o expediente, em finais de semana ou feriados, a critério da CONTRATANTE;

2.18.4. O suporte técnico da CONTRATANTE deverá ser prestado para cada componente da solução adquirida e será acionada em caso de qualquer indisponibilidade da solução.

2.18.5. Os serviços de manutenção preventiva e corretiva deverão ser executados no ambiente da CONTRATANTE;

2.18.6. As manutenções serão solicitadas através de chamado ou por notificação automática de detecção de alarme, inoperância, falhas que possam ocasionar a indisponibilidade do serviço;

2.18.7. Deverá implantar novas versões, aplicar patches de atualização, documentar e prestar suporte técnico especializado durante a vigência do contrato;

2.18.8. Toda atividade executada pela CONTRATADA deverá ser entregue documentação ao responsável técnico da CONTRATANTE, em até 72 horas, após a demanda para aceite;

2.18.9. Responder, formalmente, dentro de 03 (três) dias úteis, a todas as correspondências emitidas pela CONTRATANTE, prestando todos os esclarecimentos solicitados;

2.18.10. A CONTRATADA será responsável por todas as atividades referentes ao reposicionamento lógico e físico da solução de proteção de perímetro (ex. migração de posicionamento externo para interno, modificação na topologia de rede etc.), sempre que demandada pela CONTRATANTE;

2.18.11. A CONTRATADA deverá prestar todo o apoio necessário para garantir o funcionamento das soluções a partir da abertura de chamado, através de Central de Atendimento (número telefônico e site na Internet), fornecendo, no momento da abertura do chamado, o número, data e hora, devendo possibilitar a indicação

do nível de prioridade para o mesmo. Este será considerado o início para contagem dos prazos estabelecidos nos itens seguintes. No caso da central de chamados da CONTRATADA encontrar-se fora do município do Rio de Janeiro, esta deverá oferecer número de telefone de Discagem Direta Gratuita (DDG);

2.18.12. A CONTRATADA deverá possuir “web site” na INTERNET, com visão para os profissionais indicados pela CONTRATANTE, com os recursos mínimos de: acompanhamento do status do chamado, medidas tomadas, pendências e emissão de relatórios de chamados técnicos;

2.18.13. Todos os chamados com referência aos componentes, deverão seguir as seguintes premissas:

2.18.13.1. Os chamados poderão ser abertos durante todo o período do dia, incluindo sábados, domingos e feriados, no regime de 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana;

2.18.13.2. A CONTRATADA se obrigará a resolver problemas técnicos, on-site, caso seja necessário, dentro dos prazos estipulados no Acordo de Nível de Serviço deste TR, com todos os ônus para deslocamento e de hospedagem ser da CONTRATADA, quando ocorrer indisponibilidade da solução adquirida e inviabilidade de solução remota;

2.18.13.3. A CONTRATADA se obrigará a informar as atualizações de softwares, em até 48 horas após disponibilização pelo fabricante, para análise de criticidade, que definirá o modelo de manutenção preventiva a ser seguido, e acordado com a CONTRATANTE.

2.18.14. Fica estabelecido o seguinte Acordo de Nível de Serviço (SLA) para a prestação de suporte técnico especializado.

Severidade	Critério de Classificação do Contratante	Tempo de Resposta	Tempo de Solução
Alto Impacto	Serviço indisponível ou seriamente comprometido	Até 2 horas	Até 8 horas
Médio Impacto	Operando com Restrições	Até 4 horas	Até 12 horas
Impacto reduzido	Restrição pontual em funcionalidade	Até 8 horas	Até 24 horas

2.18.15. A CONTRATANTE deverá informar as pessoas autorizadas a abrir e fechar chamados junto à CONTRATADA, bem como o meio pelo qual a autorização de fechamento será formalizada;

2.18.16. A CONTRATANTE poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do contrato. A CONTRATADA deverá disponibilizar garantia técnica prestada pelo fabricante dos produtos oferecidos, a fim de garantir os serviços à CONRATANTE;

2.18.17. A CONTRATADA deverá disponibilizar, quando da formalização da contratação, um gerente de serviço, responsável técnico por realizar o acompanhamento periódico dos serviços prestados, com visitas para promover interações com o responsável técnico da CONTRATANTE, atuando preventivamente, com o acompanhamento dos serviços prestados, identificando necessidades, fornecendo feedbacks para melhoria do serviço prestado;

2.18.18. A CONTRATADA deverá participar ativamente das possíveis atualizações/migrações de novas versões da solução oferecida, ou mesmo do reposicionamento destas, sempre que demandada pela CONTRATANTE, seguindo plano de ações que possua, pelo menos, as fases descritas abaixo:

I. Levantamento;
II. Planejamento;
III. Homologação;
IV. Execução;
V. Operação assistida;
VI. Conclusão;

2.18.19. A CONTRATADA deve comunicar, imediatamente, por escrito, quaisquer dificuldades encontradas pelos técnicos alocados para execução dos serviços que, eventualmente, possam prejudicar a boa e pontual execução dos trabalhos, pactuando-se como INEXISTENTE as dificuldades não formalizadas de imediato.

3. DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

A presente contratação tem fundamento na Lei 10.520/2002 e no Regulamento de Licitações e Contratos da IplanRio – RLC IPLANRIO.

4. DA QUALIFICAÇÃO TÉCNICA

4.1. Prova de aptidão da empresa licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, por meio de certidão(ões) ou atestado(s), fornecido(s) por pessoa jurídica de direito público ou privado.

4.1.1. Considera-se compatível com o objeto da licitação o fornecimento de 50% do Lote 1 e ter prestado pelo menos 01 (um) serviço do Lote 2 constante na tabela 1 do item 2 deste Termo de Referência

4.1.2. Não será admitida a apresentação de atestado de capacidade técnica emitido por empresa ou empresas do mesmo grupo econômico em favor da licitante participante, no caso desta também pertencer ao grupo econômico.

4.1.3. Será admitida a soma dos atestados ou certidões apresentados pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

5. DAS OBRIGAÇÕES DA CONTRATANTE

5.1. Realizar os pagamentos na forma e condições previstas;

5.2. Realizar a fiscalização do objeto deste Termo de Referência.

6. DAS OBRIGAÇÕES DA CONTRATADA

6.1. Realizar os serviços de acordo com todas as exigências contidas no Termo de Referência e na proposta;

6.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;

6.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas e da comprovação de sua culpa ou dolo na execução do contrato;

6.4. Atender às determinações e exigências formuladas pela CONTRATANTE;

6.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, efeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo determinado pela Fiscalização;

6.6. Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão de obra necessária à completa execução dos serviços:

a) em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão do Município do Rio de Janeiro ou da CONTRATANTE como responsável subsidiário ou solidário, a CONTRATANTE poderá reter, das parcelas vincendas, o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

b) no caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária da CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

c) as retenções previstas nas alíneas “a” e “b” poderão ser realizadas tão logo tenha ciência o Município do Rio de Janeiro ou a CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o Município do Rio de Janeiro ou entidade da Administração Pública indireta sejam compelidos a tanto, administrativa ou judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA;

d) eventuais retenções previstas nas alíneas “a” e “b” somente serão liberadas pela CONTRATANTE se houver justa causa devidamente fundamentada.

6.7. Manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;

6.8. Responsabilizar-se, na forma do Contrato, pela qualidade dos serviços executados e dos materiais empregados, em conformidade com as especificações do Termo de Referência, com as normas da Associação Brasileira de Normas Técnicas – ABNT, e demais normas técnicas pertinentes, a ser atestada pelos responsáveis pela fiscalização da execução do contrato, assim como pelo refazimento do serviço e a substituição dos materiais recusados, sem ônus para o(a) CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis;

6.9. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

6.10. Indicar, nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.

6.11. Entregar os bens de acordo com todas as exigências contidas no Termo de Referência;

7. DO LOCAL DE PRESTAÇÃO DOS SERVIÇOS E DE ENTREGA DO(S) MATERIAL (IS)/EQUIPAMENTO (S)

O (s) serviço (s) deverá (ão) ser prestado (s) e a entrega do (s) material (is)/equipamento (s) deverão ser realizados no seguinte endereço: R. Afonso Cavalcanti 455 – Anexo – Sala 307 – Cidade Nova – Rio de Janeiro – RJ - CEP 20211-110.

8. DOS PRAZOS

8.1. O prazo de vigência da contratação do LOTE 1 será de 24 (vinte e quatro) meses, contados a partir da assinatura do contrato, podendo o ITEM 2 ser prorrogado, nos termos da legislação em vigor.

8.2. O prazo de vigência da contratação do LOTE 2 será de 24 (vinte e quatro) meses, contados da assinatura do contrato, podendo ser prorrogado, nos termos da legislação em vigor.

8.2.1. Caso a **CONTRATADA** tenha sido vencedora dos dois lotes, **o** prazo de vigência da contratação do Lote 2 terá início a partir da emissão de aceite da instalação das licenças e pelo prazo de vigência remanescente da contratação do Lote 1.

8.3. O prazo de entrega do (s) material (is)/equipamento (s) será de até 60 (sessenta) dias úteis, a contar da data de assinatura do contrato, podendo ser prorrogado a critério da CONTRATANTE.

8.4. O prazo de instalação e configuração da solução será de até 30 (trinta) dias úteis, a contar da data da entrega do (s) material (is)/equipamento (s), podendo ser prorrogado a critério da CONTRATANTE.

9. DA GARANTIA CONTRATUAL

9.1. A CONTRATADA prestará garantia de 2% (dois por cento) do valor total do Contrato, como determina o art. 457 do RGCAF, a ser prestada antes do ato de assinatura, em uma das modalidades previstas no art. 445 do RGCAF e no art. 81 do Decreto Municipal n.º 44.698/2018. Seus reforços poderão ser igualmente prestados nas mesmas modalidades. Caso o fornecedor escolha a modalidade seguro-garantia, esta deverá incluir a cobertura das multas eventualmente aplicadas, e, caso escolha a modalidade carta-fiança, deverá observar as regras descritas na legislação municipal aplicável a cada CONTRATANTE.

9.2. A CONTRATANTE se utilizará da garantia para assegurar as obrigações associadas à contratação, podendo recorrer a esta inclusive para cobrar valores de multas eventualmente aplicadas e ressarcir-se dos prejuízos que lhe forem causados em virtude do descumprimento das referidas obrigações. Para reparar esses prejuízos, poderá a CONTRATANTE ainda reter créditos.

9.3. Os valores das multas impostas por descumprimento das obrigações assumidas na contratação serão descontados da garantia caso não venham a ser quitados no prazo de 03 (três) dias úteis, contados da ciência da aplicação da penalidade. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

9.4. Em caso de rescisão decorrente de falta imputável à CONTRATADA, a garantia reverterá integralmente à CONTRATANTE, que promoverá a cobrança de eventual diferença que venha a ser apurada entre o importe da garantia prestada e o débito verificado.

9.5. Na hipótese de descontos da garantia a qualquer título, seu valor original deverá ser integralmente recomposto no prazo de 7 (sete) dias úteis, exceto no caso da cobrança de valores de multas aplicadas, em que esse será de 48 (quarenta e oito) horas, sempre contados da utilização ou da notificação pela CONTRATANTE, o que ocorrer por último, sob pena de rescisão administrativa do Contrato.

9.6. Caso o valor da contratação seja alterado, de acordo com o art. 92 do Decreto Municipal 44.698/2018, a CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois por cento) do valor do Contrato.

9.7. Sempre que houver reajuste ou alteração do valor da contratação, a garantia será complementada no prazo de 7 (sete) dias úteis do recebimento, pela CONTRATADA, do correspondente aviso, sob pena de aplicação das sanções previstas no RGCAF.

9.8. A garantia contratual só será liberada ou restituída com o integral cumprimento da contratação, mediante ato liberatório da autoridade contratante, de acordo com o art. 465 do RGCAF e, quando em dinheiro, atualizada monetariamente.

10. DA FISCALIZAÇÃO E ACEITE DO OBJETO

10.1. A CONTRATADA submeter-se-á a todas as medidas e procedimentos de Fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pela CONTRATANTE e/ou por seus prepostos, não eximem a CONTRATADA de suas obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais.

10.2. A Fiscalização da execução do (s) serviço (s) e da entrega dos bens caberá à comissão designada por ato da autoridade competente no âmbito da CONTRATANTE. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.

10.3. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pela CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem considerados necessários ao desempenho de suas atividades.

10.4. A CONTRATADA se obriga a permitir que o pessoal da fiscalização da CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas aos equipamentos, pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato.

10.5. Compete à CONTRATADA fazer minucioso exame das especificações do (s) serviço (s) e dos bens, de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do Contrato. O silêncio implica total aceitação das condições estabelecidas.

10.6. A atuação fiscalizadora em nada restringirá a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne aos serviço (s) contratado (s) e bens adquiridos, à sua execução e à entrega e às consequências e implicações, próximas ou remotas, perante a CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução contratual não implicará corresponsabilidade da CONTRATANTE ou de seus prepostos.

10.7. A aceitação do objeto deste Termo de Referência se dará mediante a avaliação de Comissão de Fiscalização designada pela autoridade competente no âmbito da CONTRATANTE, e constituída na forma do art. 501, do RGCAF, que constatará se os serviços executados e os bens fornecidos atendem a todas as especificações contidas neste Termo de Referência ou no processo que ensejou a presente contratação.

10.8. O objeto do presente Termo de Referência será recebido em tantas parcelas quantas forem às relativas ao pagamento.

10.9. Os serviços e bens cujos padrões de qualidade estejam em desacordo com a especificação deste Termo de Referência e seus anexos deverão ser recusados pela Comissão responsável pela fiscalização do contrato, que anotará em registro próprio as ocorrências e determinará o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 5 (cinco) dias, para ratificação.

10.10. Na hipótese de recusa de aceitação, por não atenderem às exigências da CONTRATANTE, a CONTRATADA deverá reexecutar ou substituir quaisquer serviços e bens defeituosos ou qualitativamente inferiores, passando a contar os prazos para pagamento e demais compromissos da CONTRATANTE da data da efetiva aceitação. Caso a CONTRATADA não reexecute os serviços não aceitos no prazo assinado ou substitua os bens não aceitos no prazo assinado, a CONTRATANTE se reserva o direito de providenciar sua execução ou seu fornecimento às expensas da CONTRATADA, sem prejuízo das penalidades cabíveis.

10.11. O Aceite Provisório ficará a cargo da Comissão de Fiscalização, que emitirá Termo de Aceitação Provisória em até 05 (cinco), após a entrega da Solução instalada e configurada.

11. DAS CONDIÇÕES DE PAGAMENTO

11.1. Em relação ao Lote 1 da tabela 1 do item 2, o pagamento será efetuado integralmente à CONTRATADA após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.

11.1.1. O pagamento à CONTRATADA será realizado em razão do efetivo fornecimento realizado e aceito, sem que a CONTRATANTE esteja obrigado(a) a pagar o valor total do contrato caso todo o quantitativo do objeto não tenha sido regularmente entregue e aceito.

11.2. Em relação ao Lote 2 da tabela 1, o(s) pagamento(s) será(ão) efetuado(s) mensalmente à CONTRATADA após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.

11.3. Para fins de medição, se for o caso, e faturamento, o período-base de medição do serviço prestado será de um mês, considerando-se o mês civil, podendo no primeiro mês e no último, para fins de acerto de contas, o período se constituir em fração do mês, considerado para esse fim o mês com 30 (trinta) dias.

11.4. O pagamento à CONTRATADA será realizado em razão dos serviços efetivamente prestados e aceitos no período-base mencionado no item anterior sem que o(a) CONTRATANTE esteja obrigado(a) a pagar o valor total do Contrato.

11.5. A CONTRATADA deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista, na forma do Anexo do Edital.

11.6. O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à CONTRATADA, sofrerá a incidência de juros calculados de acordo com a variação da Taxa Selic, pro rata die entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança no setor competente da CONTRATANTE e a data do efetivo pagamento, limitado ao percentual de 12% (doze por cento) ao ano.

11.7. O valor dos pagamentos eventualmente antecipados será descontado à taxa de 1% (um por cento) ao mês, calculada pro rata die, entre o dia do pagamento e o 30º (trigésimo) dia da data do protocolo do documento de cobrança no setor competente do (a) CONTRATANTE.

11.8. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. Pelo descumprimento total ou parcial da Ata de Registro de Preços ou do Contrato, o Órgão Gerenciador e os (as) CONTRATANTES, respectivamente, poderão, sem prejuízo responsabilidade civil e criminal que couber, aplicar as seguintes sanções, previstas nos artigos 7º da Lei Federal nº 10.520/02 no art. 589 do RGCAF e Regulamento de Licitações e Contratos da Contratante, garantida a defesa prévia ao contratado:

I - advertência;

II - Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;

III - Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso, e, respectivamente, nas hipóteses de descumprimento total ou parcial da obrigação, inclusive nos casos de rescisão por culpa da CONTRATADA;

IV - suspensão temporária do direito de licitar e impedimento de contratar com a Administração Municipal;

12.2. A multa aplicada será depositada em conta bancária indicada pela IplanRio, descontada dos pagamentos eventualmente devidos, descontada da garantia ou cobrada judicialmente.

12.3. As sanções previstas nos incisos I e IV do subitem 12.1 poderão ser aplicadas juntamente com as dos incisos II e III, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis e não excluem a possibilidade de rescisão unilateral do contrato;

12.4. Do ato que aplicar a pena prevista no inciso IV do subitem 14.1, a autoridade competente no âmbito da CONTRATANTE dará conhecimento aos demais órgãos e entidades municipais interessados, na página oficial desta empresa pública na internet.

12.5. A sanção prevista no inciso IV do subitem 12.1 poderá também ser aplicada às empresas ou aos profissionais que, em razão dos contratos regidos pelo Decreto Municipal n.º 44.698/2018:

I - tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II - tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

III - demonstrem não possuir idoneidade para contratar com a IplanRio em virtude de atos ilícitos praticados.

12.6. As multas previstas nos incisos II e III do subitem 12.1 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.

12.7. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.

12.8. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

13. DA MATRIZ DE RISCOS

13.1. Para a presente contratação foram identificados os principais riscos conhecidos na Matriz constante do Anexo I deste Termo de Referência, bem como estabelecidos os respectivos responsáveis e descritas suas respostas sugeridas.

13.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na Matriz de Riscos como sendo de responsabilidade da CONTRATADA.

13.3. Sempre que atendidas as condições do contrato e mantidas as disposições da Matriz de Risco, considera-se mantido o equilíbrio econômico-financeiro.

13.4. A proposta comercial deverá ser elaborada levando em consideração a natureza e a extensão dos riscos relacionados na Matriz de Risco.

14. DA PROPOSTA DE PREÇOS

14.1. A pretensa CONTRATADA deverá apresentar proposta de preços de acordo com as especificações deste Termo de Referência e nos moldes praticados pelo Município do Rio de Janeiro.

14.2. Os preços propostos deverão estar de acordo com os praticados no mercado, em moeda nacional (Reais) e neles deverão estar inclusos todos os impostos, taxas, fretes, material, mão de obra, instalações e quaisquer outras despesas necessárias e não especificadas neste Termo de Referência, mas julgadas essenciais ao cumprimento do objeto desta contratação, observando-se, ainda, o contido no subitem 13.4 deste Termo de Referência.

15. DO TIPO DE LICITAÇÃO

15.1. O tipo de licitação será o menor preço por Lote.

16. DA PROTEÇÃO DE DADOS PESSOAIS

16.1. Havendo tratamento de dados pessoais no desenvolvimento de quaisquer atividades relacionadas com o objeto, as Partes observarão a Legislação de Privacidade e de Proteção de Dados Pessoais, em especial, a Lei 13.709/2018 (LGPD).

Rio de Janeiro, 12 de abril de 2022.

_____
Ricardo Rodrigues da Silva
Supervisor
Diretoria de Operações
IplanRio

_____
Luciana Nascimento Santos
Gerente de Infraestrutura Tecnológica
Diretoria de Operações
IplanRio

Aprovo,

_____
Jorge Francisco Antunes
Diretor de Operações
IplanRio