Governo do Estado de
RONDÔNIA

Departamento Estadual de Estradas de Rodagem e Transportes - DER

CONTRATO Nº 059/2021/PJ/DER-RO

CONTRATO Nº 059/2021/PJ/DER-RO

CONTRATO QUE ENTRE SI CELEBRAM O DEPARTAMENTO ESTADUAL DE ESTRADAS DE RODAGEM E TRANSPORTES/DER-RO E NBS SERVICOS DE COMUNICACOES LTDA, PARA OS FINS QUE ESPECIFICAM.

Aos dezenove dias do mês de agosto do ano de dois mil e vinte e um o **DEPARTAMENTO ESTADUAL DE ESTRADAS DE RODAGEM E TRANSPORTES/DER-RO**, inscrito no CGC (MF) sob o n.º 04-285.920/0001-54, com sede à Avenida Farquar, 2986, complexo Rio Madeira, Anexo Rio Jamari, 4º e 5º Andar, Bairro Pedrinhas, CEP: 76.803-470, Porto Velho-RO, doravante designado **DER-RO**, neste ato representado por seu Diretor Geral, o **Sr. ELIAS REZENDE DE OLIVEIRA,** portador do RG nº 518.664 SSP/RO e CPF nº 497.642.922-91, conforme Decreto de 19 de junho de 2020, DOE edição 120, de 23 de junho de 2020 e **NBS SERVICOS DE COMUNICACOES LTDA,** CNPJ/MF n.º 26.824.572/0001-89, estabelecida na Rua João dos Santos Filho, Bairro Dois de Abril, nº 123, na cidade de Ji-Paraná/RO, doravante denominada **CONTRATADA**, neste ato representada pelo seu Administrador, o **Sr. JULIANO MURILO COCO,** CPF nº 003.747.089-24, celebram o presente Contrato, decorrente do **PROCESSO ADMINISTRATIVO Nº 0009.365939/2020-99**, o qual originou o **PROCEDIMENTO DE ADESÃO A ATA DE REGISTRO DE PREÇOS nº 080/2021, Referente ao Pregão Eletrônico 280/2020/ALFA/SUPEL**, homologado pela Autoridade Competente, nos termos da Lei 8.666/93, Decreto 7.892/13, e art. 26 e 27 do Decreto Estadual nº 18.340/2013, sujeitando-se às normas dos supramencionados diplomas legais, mediante as cláusulas e condições a seguir estabelecidas:

CLÁUSULA PRIMEIRA – DO OBJETO

PARÁGRAFO ÚNICO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇO DE TRANSMISSÃO DE DADOS E SOLUÇÃO DE SEGURANÇA, devidamente autorizada pela Agência Nacional de Telecomunicações – ANATEL, para prestação de serviços de acesso à Internet, utilizando protocolo IP/MPLS, para formar a Rede WAN do DEPARTAMENTO ESTADUAL DE ESTRADAS DE RODAGEM E TRANSPORTES -DER e Residências Regionais - DER de forma permanente, dedicada e exclusiva, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados.

CLÁUSULA SEGUNDA – ESPECIFICAÇÃO TÉCNICA, DA ENTREGA E RECEBIMENTO, GARANTIA, LOCAL DE UTILIZAÇÃO/DESTINAÇÃO DO BEM

PARÁGRAFO PRIMEIRO - ESPECIFICAÇÃO TÉCNICA:

1. A contratação do referido objeto será de acordo com as condições, exigências e quantidades estabelecidas neste item, conforme abaixo:

Lote Único

Item	Descrição	Velocidade	QUANTIDADE
1	Link de internet dedicada com 14 IPs públicos	100 Mbps	2
2	Concentrador MPLS	5000 Mbps	1
4	Comunicação de Dados Terrestres (MPLS)	100 Mbps	16

2. ESPECIFICAÇÃO DO OBJETO

Item	Velocidade/Link	Unidade	Município	Quant.
1	Link de internet dedicada com 14 IPs públicos, com banda de velocidade100 Mbps Link/Ano.	DER-CPA	Porto Velho	2
2	Concentrador MPLS, com banda de velocidade 5 Gbps Link/ Ano.	DER-CPA	Porto Velho	1
3	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	7º Residência Regional - DER	Alvorada do Oeste	1
4	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	15º Residência Regional - DER	Buritis	1
5	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	4º Residência Regional - DER	Cacoal	1
6	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	Aeroporto - DER	Cacoal	1
7	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	1º Residência Regional - DER	Colorado do Oeste	1
8	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	12º Residência Regional - DER	Jaru	1
9	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	Usina de Asfalto - DER	Jaru	1
10	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	8º Residência Regional - DER	Ji-Paraná	1
11	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	Aeroporto - DER	Ji-Paraná	1
12	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	6º Residência Regional - DER	Machadinho do Oeste	1
13	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	3º Residência Regional - DER	Ouro Preto do Oeste	1

14	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	11º Residência Regional - DER	Pimenta Bueno	1
15	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	5º Residência Regional - DER	Rolim de Moura	1
16	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	Usina de Asfalto - DER	Rolim de Moura	1
17	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	16º Residência Regional - DER	São Francisco	1
18	Comunicação de Dados Terrestres (MPLS), com banda de velocidade 100Mbps Link/Ano	9º Residência Regional - DER	Vilhena	1

3. EQUIPAMENTO DE CPE'S - Customer premises equipment.

3.1. Deverá ser disponibilizado, pela Contratada, juntamente com a rede de comunicação de dados, equipamentos CPE's (Customer premises equipment) com SNMP v.2, para a rede WAN DER-RO vinculados à contratação dos correspondentes serviços de acesso, com as seguintes características básicas:

3.2. O Equipamento deverá possuir, no mínimo, as seguintes características técnicas:

Característica	**Detalhes**
Auto-negotiation	Possuir no mínimo, 2 (duas) interfaces GigabitEthernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u.
	Deve suportar a inserção de interfaces analógicas (FXS ou FXO).
	Deve possuir no mínimo dois slot(s) internos para inserção de DSPs (Digital Signal Processor).
WAN	1 (uma) porta de WAN que possa conectar aos dispositivos de acesso, podendo ser interface G.SHDSL, ADSL, V.35 entre outras.
Performance	Performance mínima de 320.000 pps com pacotes de 64 bytes.
Capacidade	Memória mínima DRAM de 512MB e memória Flash de 256MB.
Energia	Fonte de alimentação 110/220V.
Gerenciamento	Command Line Interface (CLI),Telnet e Console, SNMP v1/v2/v3 e RMON .
Protocolos	Deve Suportar o protocolo HDLC e Frame Relay.
	Deve possuir suporte ao protocolo PPP (incluindo PPP sobre ATM, PPP sobre Frame Relay e PPP sobre Ethernet.
	Deve implementar o protocolo VRRP e suportar os protocolos de IP Multicast: IGMP e PIM.
Roteamento	Suportar o protocolo roteável IP, roteamento estático, OSPFv2 e BGPv4.
QoS	Deve suportar a classificação de pacotes de dados (QoS) baseados em Layer 3 ou Layer

	4.
Segurança	Deve possuir suporte a autenticação de usuário através de RADIUS e TACACS.
	Possuir aceleração criptografica por hardware para as certificações DES, 3DES e AES.
	Deve suportar via licença adicional ou upgrade de software no mínimo as seguintes funcionalidades: - suportar serviços de VPN baseado no padrão IPSEC; - suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC; - suportar a concentração de VPNs (IPSEC) para acessos remotos; - suportar a concentração de SSL-VPNs para acessos remotos; - suportar a autenticação e autorização de usuários para acesso VPN; - suportar operação como Firewall Transparente ;

4. DA COMPROVAÇÃO E QUANTIDADE ESTIMADA

4.1. A quantidade estimada para o objeto a ser contratado, encontra-se base no artigo 15 § 7, inciso II, da Lei 8.666/93, nessa esteira, justifica-se a contratação supracitada pelas razões e fundamentos abaixo esposados em consonância com a justificação da Gerencia solicitante dos serviços:

4.2. O Consumo do quantitativo ATUAL DE 10MBS por distribuição INTERNET CONECCT com o quantitativo insuficiente para atender todas as demandas de serviços de dados da DEPARTAMENTO ESTADUAL DE ESTRADAS DE RODAGEM E TRANSPORTES -DER.

4.3. Cada unidade de Residência Regional tem como média o quantitativo de 10 (dez) usuários conectados, sendo que unidades maiores como Ji-Paraná este número de DESKTOP conectados a internet chega ao número 20 (vinte) usuários na sequencia esta a Residência de Rolim de Moura com 16 usuários.

4.4. Dividindo o quantitativo de 10MB por número total de usuários, Referência (10 dez), temos como resultado uma velocidade média de conexão por usuário de 1MBps, o que é insuficiente e inadmissível ao GOVERNO DO ESTADO DE RONDÔNIA, pois as ferramentas que são ofertadas pelo GOVERNO, como uso do SEI, necessita de conexão a internet de BANDA LARGA, suficiente para todos os procedimentos na plataforma Eletrônica de Informação, com este velocidade de 1MBps os usuários das residências regionais não conseguem, anexar documentos satisfatoriamente, não conseguem inserir ou consultar documentos no servidor de Pasta Compartilhada, não conseguem realizar videoconferência satisfatoriamente, o que tem gerado custos elevados ao GOVERNO DO ESTADO DE RONDÔNIA, com envio de documentos físicos via Malote para a Capital Porto Velho, além do consumo de papel, de toners e suas burocracias, assim sendo as atividades devido a internet limitada, não é sustentável ao Governo, e não está de acordo com a política GOVERNO SEM PAPEL, através do Sistema Eletrônico de Informação - SEI.

4.5. Ao comparar a velocidade de conexão exposta aos usuários das unidades regionais do DER no interior como exposto no item acima 3.4.3, com os usuários de Porto Velho, que trabalham no Palácio Rio Madeira, que são beneficiados pela INFOVIA, cada usuário no Palácio Rio Madeira, navega há uma velocidade de até 100 MB, o que é superior um único usuário trafegar há uma velocidade superior, somando todas as unidades regionais do DER no interior.

4.6. Hoje os serviços de dados disponíveis no consumo atual é insuficiente aos usuários, e só tem causado transtornos, e custos ao DER.

a) -Serviço de acesso dedicado à Internet com Proteção em Backbone contra-ataques DDoS - Velocidade de 200 Mbps.

Trata-se do link de redundância no Palácio Rio Madeira que necessita de disponibilidade 24 horas por dia x 7 por semana.

b) - Serviço de Transmissão de dados - Rede MPLS - Concentrador - Velocidade 5000 Mbps

Trata-se do concentrador de link de internet disponibilizado a todas unidades regionais da DER no interior, ou seja, é o valor de 5000 Mbps dividido pelo total de municípios atendidos, conforme os itens 3 ao 18, sendo como total a velocidade média de 300 Mbps por unidade.

c) - Serviço de Transmissão de dados - Rede MPLS - 100 Mbps

c.1 - É o resultado do total de municípios após a divisão do Concentrador, pelo total de municípios, ou seja, Porto Velho, concentrador 5000 Mbps, com instalação de equipamentos, e no interior em cada unidade com instalação de equipamentos que comunicam-se entre si, e permite a todos os usuários navegarem em rede interna.

c.2 - Conforme exposto no item 3.4.3, com a contratação ideal do quantitativo exposto, cada unidade regional do DER, terá uma velocidade mínima satisfatória com média de velocidade por usuário de 10 Mbps, o que é ainda muito inferior a velocidade que os usuários utilizam na capital, mas é a velocidade ideal e satisfatória.

d) - CPE - (FIREWALL UTM)

CPE - Customer premises equipment. Trata-se de recomendação da Estado para Resultados - EPR, que todas as contratações de serviço de dados tenha sistema de Firewall, como procedimento de seguranças aos órgãos e usuários. Com a combinação do *software* e de *hardware* de proteção, é chamado tecnicamente de "appliance" que controlam o fluxo de entrada e saída de informações protegendo dados e informações do Governo do Estado de Rondônia.

5. SOLUÇÃO DE SEGURANÇA GERENCIADA (CPE):

5.1. A Solução de Segurança Deverá Possuir as Seguintes Características Técnicas:

5.2. APPLIANCE DE 20GBPS DE CAPACIDADE DE FIREWALL - UTM

5.2.1. CARACTERÍSTICAS DO HARDWARE

- Possuir throughput mínimo de 20Gbps;
- Suportar no mínimo 6 milhões conexões simultâneas;
- Suportar no mínimo 70.000 mil novas conexões por Segundo;
- Throughput de, no mínimo, 2.5 Gbps com as seguintes funcionalidades habilitadas simultaneamente: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
- Estar licenciado para, ou suportar sem o uso de licença, 2 mil túneis de VPN IPSec Site-to-Site simultâneos;
- O equipamento deve possuir, pelo menos, 10 interfaces, sendo no mínimo 8 interfaces 1Gbps com RJ-45;
- Deve suportar, 2 interfaces 10Gbps com SFP+;
- Deve suportar, 4 interfaces 1Gbps com SFP;
- Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;
- Deve possuir armazenamento interno, no mínimo, de 240GB em SSD;
- Possuir suporte e estar licenciado a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação padrão C13/C14;

- A alimentação dos equipamentos deve ser automática de 100-240V em 60Hz;
- Deve possuir fonte redundante “Hot Swappable”;
- Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo é desligado ou não responde. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração de instancias via software.
- Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos.

5.3. ESPECIFICAÇÕES GERIAS DE SOFTWARE

5.3.1. FUNÇÕES BÁSICAS

- Hardware (Appliances) que atuam na segurança e performance do ambiente de rede; VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
- Controle de Aplicações;
- Proxy Web e Filtro de Conteúdo Web (URL Filtering); Detecção e prevenção de intrusos – IPS;
- Qualidade de serviço – QOS;
- Anti-Malware;
- Cluster.

5.4. CARACTERÍSTICAS GERAIS

- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; Interface em português ou inglês;
- O sistema deve permitir o acesso à interface de gerenciamento por qualquer interface de rede configurada.
- O Software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
- Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
- Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v2 e v3.
- A Solução deverá prover inspeção SSL:
- A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.
- Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;
- Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.
- Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

5.5. DAS FUNCIONALIDADES DO FIREWALL

- Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;
- Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças;

- Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;
- O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente;
- As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;
- Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata;
- Deve permitir habilitar ou desabilitar o registro de log por política de firewall;
- Possuir controle de acesso à internet por endereço IP de origem e destino;
- Possuir controle de acesso à internet por sub-rede;
- Possuir suporte a tags de VLAN (802.1q);
- Suportar agregação de links, segundo padrão IEEE 802.3ad);
- Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;
- Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um;
- Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
- Possuir suporte a roteamento dinâmico RIP, OSPF, BGP;
- Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- Deverá suportar aplicações multimídia como: H.323, SIP;
- Possuir tecnologia de firewall do tipo Stateful;
- Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- Permitir o funcionamento em modo transparente tipo “bridge”;
- Permitir a criação de VLANS no padrão IEEE 802.1q;
- A comunicação da gerencia com os gateways gerenciados deverá ser feito através de canal criptografada;
- Deverá suportar forwarding de multicast;
- Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- Permitir o agrupamento de serviços;
- Permitir o filtro de pacotes sem a utilização de NAT;
- A solução deve ter a capacidade de operar através de uma unica instancia de Firewall de forma simultânea mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);
- Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- Possuir mecanismo de anti-spoofing;

- Permitir criação de regras definidas pelo usuário;
- Possuir a funcionalidade de balanceamento e contingência de links;

5.6.IDENTIFICAÇÃO DE USUÁRIO

- Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;
- Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;
- A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;
- A solução deve suportar a opção de instalação de Softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD.

5.7.DAS FUNCIONALIDADES DA VPN

- VPN baseada em appliance;
- Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES; Suporte a certificados PKI X.509 para construção de VPNs;
- Possuir suporte a VPNs IPSec site-to-site:
- Criptografia, 3DES, AES128, AES256, AES-GCM-128 Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
- Algoritmo Internet Key Exchange (IKE) versões I e II; AES 128 e 256 (Advanced Encryption Standard);
- Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30; Possuir suporte a VPN SSL;
- Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
- A VPN SSL deve possibilitar o acesso a toda infra-estrutura da contratante de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
- Deve permitir a arquitetura de vpn hub and spoke; Suporte a VPNs IPSec client-to-site:
- Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
- Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
- Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub);
- A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis: Site-to-Site;
- Full-Mesh; Star.

5.8. DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO

- A Detecção de Intrusão deverá ser baseada em appliance:
- Capacidade de detecção de mais de 22.000 ataques;
- O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- Possuir tecnologia de detecção baseada em assinatura;
- O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
- Possuir capacidade de remontagem de pacotes para identificação de ataques;
- Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- Mecanismos de detecção/proteção de ataques;
- Reconhecimento de padrões;
- Análise de protocolos;
- Detecção de anomalias;
- Detecção de ataques de RPC (Remote procedure call);
- Proteção contra ataques de Windows ou NetBios;
- Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- Proteção contra ataques DNS (Domain Name System);
- Proteção contra ataques a FTP, SSH, Telnet e rlogin;
- Proteção contra ataques de ICMP (Internet Control Message Protocol);
- Alarmes na console de administração;
- Alertas via correio eletrônico;
- Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
- Capacidade de resposta/logs ativa a ataques;
- Terminação de sessões via TCP resets;
- Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- Possuir filtros de ataques por anomalias;
- Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- Permitir filtros de anomalias de protocolos;
- Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- Suportar verificação de ataque nas camadas de aplicação.

5.9. DAS FUNCIONALIDADES DE QOS

- Adotar solução de Qualidade de Serviço baseada em appliance;

- Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
- Permitir modificação de valores DSCP para o DiffServ;
- Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

5.10. DAS FUNCIONALIDADES DO ANTIVÍRUS

- Possuir funções de Antivírus, Anti-spyware;
- Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3 e FTP;
- Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;
- Permitir o bloqueio de download de arquivos por tamanho.

5.11. DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB

- Possuir solução de filtro de conteúdo web integrado a solução de segurança solicitada nesse documento
- Reconhecer pelo menos 3.100 (três mil e cem) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- Possuir pelo menos 110 categorias para classificação de sites web
- Possuir categorias pré definidas, no mínimo, para os seguintes tipos de sites web como:
- Anonymizer;
- Computers / Internet
- File Storage and Sharing
- Gambling
- Instant Messaging
- Media Sharing
- Media Streams
- P2P File Sharing
- Social Networking

- Pornografia;
- Transferência de arquivos;
- Chat;
- Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentava de acesso a recursos proibidos pela política de segurança da CONTRATANTE;
- Permir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;
- Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;
- Permitir a criação de listas personalizadas de URLs permidas – lista branca e bloqueadas – lista negra;
- Deverá permitir o bloqueio de URLs inválidas cujo campo CN do cerficado SSL não contém um domínio válido;
- Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;
- Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;
- Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;
- A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
- Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
- Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
- Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
- Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;
- Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;
- Suportar a criação de categorias de URLs customizadas;
- Suportar a exclusão de URLs do bloqueio, por categoria;
- Permitir a customização de página de bloqueio;

- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório do Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP, para appliance to tipo I, II, III.
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

5.12. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES

- As funcionalidades abaixo devem ser baseadas em appliance:
- Deverá reconhecer no mínimo 700 aplicações;
- Deverá possuir pelo menos 10 categorias para classificação de aplicações;
- Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:
- P2P;
- Web;
- Transferência de arquivos;
- Chat;
- Social;
- Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

5.13 SISTEMA DE PROTEÇÃO AVANÇADA CONTRA AMEAÇAS AVANÇADAS - ATP

- A solução deve suportar o envio de artefatos para ambiente controlado sandboxing em nuvem do proprio fabricante para identificação e bloqueio de ameaças direcionados e persistentes.
- A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

- Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.
- A inspeção com a funcionalidade de MTA deverá ser atendida.
- A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
- Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;
- A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010 e 2013;
- A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;
- Toda análise dos arquivos deverá ser realizada na nuvem do proprio fabricante em ambiente controlado Sandboxing. Não serão aceitas soluções em servidores ou software livre;
- A funcionalidade de prevenção de ameaças avançadas deve ser habilitada de forma independente das outras funcionalidades de segurança;
- Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;
- Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm;
- A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;
- Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:
- Número de arquivos emulados;
- Numero de arquivos com malware.
- Suportar exceção de inspeção por IP de origem ou IP de destino;
- Suportar exceção de inspeção por tipos de arquivos ;

5.14. SD-WAN

5.14.1. Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;

- Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;
- Permitir utilizar VPN IPsec para interligar unidades remotas;
- O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;
- Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;
- Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:
- Consumo de banda;
- Perda de pacotes;

- Jitter;
- Latência.

5.15. ALTA DISPONIBILIDADE

- Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.
- Não serão permitidas soluções de cluster (HA) que façam com que o equipamento (s) reinicie após qualquer modificação de parâmetro/configuração seja realizada pelo administrador.
- O Sincronismo dos servidores deve ser por interface exclusiva.

5.16. SERVIÇOS DE PRESTAÇÃO DE SUPORTE TÉCNICO REMOTO 8X5

- Serviço de suporte REMOTO para os equipamentos de segurança de borda contratados, no horário 8x5 (Segunda a sexta-feira das 08:00 às 18:00, exceto feriados), pelo tempo de contrato, com as seguintes características:
- A contratada deve possuir serviço de abertura de chamados remoto capaz de abrir chamados de forma centralizada, em caso de ocorrências de defeitos e/ou falhas na rede relativos aos equipamentos e/ou produtos fornecidos;
- A contratada deverá iniciar o atendimento de suporte em no máximo 8 horas úteis após a abertura do chamado;
- A contratada deverá fornecer atestado comprovando a existência de equipe técnica de no mínimo 3 pessoas capacitadas em todas as soluções adquiridas. O atestado deverá ser fornecido pelo fabricante;
- A CONTRATADA será eximida da aplicação das sanções administrativas para os respectivos chamados em que sejam descumpridos os tempos de solução, desde que comprovadas as seguintes situações: Quando constatado que o problema está relacionado a “bug” no produto e que o fabricante não possui uma correção imediata para tal, sendo este fato declarado pelo próprio;
- A CONTRATADA tomou todas as medidas possíveis visando providenciar solução de contorno; O suporte prevê atendimento em até 4 horas, limitados em 16 horas mensais;

5.17. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL

5.17.1. FUNCIONALIDADES DE GERENCIAMENTO

- Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;
- A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.
- O gerenciamento centralizado poderá ser entregue como appliance fisico ou virtual. Caso seja entregue em appliance fisíco deve ser compativel com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compativel com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;
- Caso a solução possua licenças relacionadas a capacidade de log e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;
- Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

- Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;
- A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou titulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;
- A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.
- Deve possibilitar a realização de “backup” e restauração de dados.
- Deve possibilitar o envio dos “logs” gerados a outro concentrador de “logs” externo a solução.
- Deve possibilitar a gerência de “logs”, realizando as configurações de relatórios de todos os “firewalls” integrados.
- Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.
- O gerenciamento deve permitir/possuir:
- Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;
- Monitoração de logs; Debugging;
- Acesso concorrente de administradores;
- Deve permitir usar palavras chaves para facilitar identificação de regras;
- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações; Autenticação integrada à base de dados local;
- Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;
- Criação de regras que fiquem ativas em horário definido;
- Backup das configurações e rollback de configuração para a última configuração salva; Habilidade de upgrade via interface de gerenciamento;
- Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;
- Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;
- Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;
- Deve permitir a criação de objetos e políticas compartilhadas;
- Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
- Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

5.18. FUNCIONALIDADES DE ANALISE DE LOG E CORRELAÇÃO DE EVENTOS

- Deve incluir uma ferramenta do próprio fabricante ou solução de terceiros para correlacionar os eventos de segurança das funcionalidades adquiridas neste edital.
- Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.
- A solução deve exportar relatórios via HTML, CSV e PDF;
- A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;
- A solução deve permitir o administrador deve ser capaz de atribuir esses filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.
- A solução deve prover no mínimo as seguintes funcionalidade para análise avançada dos incidentes:
- Visualizar quantidade de tráfego utilizado de aplicações e navegação;
- Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
- Estatísticas com comparativo de período (hora, dia e mês);
- Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais Serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;
- Deve estar incluso horários predefinidos, diários, semanais e relatórios mensais. Incluindo Top eventos, Top origem, Top destinos, Top Serviços, Top origens e os seus principais eventos, Top destinos e seus principais eventos;
- Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado.
- Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.
- Deverá prover análise de tráfego de rede de modo centralizado;
- Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:
- Análise de ameaças e incidentes de segurança;
- Análise de tráfego e uso de categorias Web;
- Análise de tráfego e uso de aplicativos;
- Análise de tráfego e ameaças por usuário;
- A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;
- Deverá possuir ferramenta para salvar consultas avançadas;
- Deve possuir relatórios personalizados;
- Deverá ser capaz de efetuar o arquivamento de relatórios;
- Deve possuir agendamento de relatórios;

5.19. SERVIÇO DE INSTALAÇÃO

- Para as soluções ofertadas, a contratada deverá cotar um valor total para a instalação e customização inicial dos dispositivos adquiridos;
- Este serviço deverá ser utilizado para a operacionalização inicial dos produtos adquiridos, customização, funcionalidades e políticas;
- A instalação deve ser feita por técnicos treinados e certificados, comprovados através de atestado emitido pelo fabricante;
- Toda a despesa de deslocamento e hospedagem deve ser de responsabilidade da contratada.
- Os serviços requeridos pela Contratante devem ser configurados e executados pela CONTRATADA.

5.20.TREINAMENTO PARA O SISTEMA DE FIREWALL UTM

- Deverá ser fornecido treinamento para a solução de firewall adquirida (hardware ou Software) para a equipe do cliente;
- A equipe de Tecnologia da Informação do DER, a receber o treinamento é de no máximo 04 pessoas;
- Carga Horária mínima de 20 horas;
- O instrutor deverá ser certificado pela fabricante dos produtos para realizar os treinamentos, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de segurança da informação;
- O material a ser fornecido no treinamento deverá ser o material certificado pelo próprio fabricante, não serão aceitas cópias de apostilas;
- Toda a infraestrutura, os custos de material (apostilas, manuais, etc.), alimentação (coffee break), instrutor (deslocamento, hospedagem e vencimentos) ficará a cargo da CONTRATADA;
- O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;
- Deverá ser fornecido um 01 lanche (coffee break) para cada 4 horas de treinamento suficiente para todos os alunos;
- Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;
- Este treinamento poderá ser realizado em ambiente externo ao da CONTRATANTE, inclusive com os recursos para laboratórios (handson) salvo em caso de necessidade e acordo entre CONTRATADA e CONTRATANTE;
- Os cursos deverão ser realizados em horários e data a serem acordados pela CONTRATADA e CONTRATANTE;
- A CONTRATADA deverá ofertar as instalações na localidade da CONTRATANTE para a realização dos treinamentos com os requisitos mínimos de infraestrutura de sala de treinamento.

6. DETALHAMENTO DOS SERVIÇOS DE INTERNET

6.1. Serviço de acesso à Rede Mundial de Computadores (Internet) com Proteção em Backbone contra ataques DDoS, através de uma conexão dedicada até o backbone da operadora, que deverá ser capaz de encaminhar 100% (cem por cento) do tráfego contratado.

6.2. Deverá ser fornecida e alocada, pela empresa CONTRATADA, uma faixa de endereçamento IP válidos para a Internet, composta por, no mínimo, 30 (trinta) endereços IPv4. Caso a CONTRATANTE necessite de mais endereços IP válidos, será feita uma solicitação formal com as devidas justificativas para a CONTRATADA, que por sua vez estará obrigada a atender as demandas da CONTRATANTE;

6.3. Parâmetros de Qualidade e Níveis de Serviço (SLA).

- Disponibilidade mínima mensal de 99,6%;

- Taxa de erros máxima admitida de 10^{-6};
- Latência máxima entre o acesso e o backbone da CONTRATADA de 50ms;

6.4. Tempo máximo para mudança de velocidade de 30 (trinta) dias corridos a partir da data de solicitação, interrompendo o serviço por no máximo 1 (uma) hora;

6.5. Tempo máximo para mudança de endereço de 30 (trinta) dias corridos a partir da data de solicitação, mantendo o acesso antigo em funcionamento até 2 (duas) horas antes da ativação do novo acesso no novo endereço;

6.6. Tempo máximo para mudança de tecnologia de acesso de 30 (trinta) dias corridos a partir da data de solicitação, interrompendo o serviço por no máximo 1(uma) hora;

6.7. Prazo para recuperação/reparação do serviço (normalização do serviço após o registro da degradação, falha, defeito e/ou paralisação): no máximo 6 (seis) horas para todos os municípios.

6.8. O acesso à Internet (circuito de dados) não poderá ser subcontratado de terceiros, devendo a CONTRATADA fornecer ambos os serviços.

7. DETALHAMENTO DOS SERVIÇOS DE INTRANET

7.1. Os serviços de Intranet são os acessos à Rede Virtual Privada (VPN), a ser criada pela CONTRATADA em seu backbone IP/MPLS, por onde fruirá o tráfego de dados entre as diversas unidades do CONTRATANTE, garantindo segurança e privacidade das informações trafegadas.

7.2. O serviço deverá ser instalado na velocidade indicada como INICIAL. A alteração para a velocidade FUTURA ocorrerá mediante solicitação prévia do CONTRATANTE e em conformidade com os prazos e preços definidos no contrato;

7.3. Garantir o roteamento das conexões dedicadas utilizando protocolo MPLS – Multiprotocol Label Switching.

7.4. Cada acesso não poderá ser compartilhado com nenhum outro cliente da CONTRATADA e deverá ser capaz de absorver 100% (cem por cento) do tráfego referente à velocidade contratada;

7.5. Operar em conformidade com, no mínimo, as seguintes RFCs:

- RFC 3031: “Multiprotocol Label Switching Architecture”;
- RFC 3032: “MPLS Label Stack Encoding”;
- RFC 3270: “Multi-Protocol Label Switching (MPLS) Support of Differentiated Services”;
- RFC 2474: “Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers”;
- RFC 2475: “An Architecture for Differentiated Services”;

7.6. Os equipamentos instalados em todos os acessos da rede deverão realizar a marcação de pacotes com vistas à priorização de dados provenientes dos seguintes aplicativos:

7.6.1. Permitir a classificação e marcação de diferentes níveis de tráfego (CoS e QoS), sendo implementadas as seguintes classes de serviço:

- **Tempo Real Voz e/ou Vídeo**: Aplicações sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem a priorização de pacotes de dados e reserva de banda na rede;
- **Dados Prioritários**: Aplicações interativas, que exigem entrega garantida e tratamento prioritário. São os dados envolvidos nas aplicações essenciais às atividades fins do CONTRATANTE:
- **Dados Comuns (mínimo 25% da banda total do acesso)**: Aplicações com mensagens de tamanho muito variado e não imprescindíveis às atividades fins do CONTRATANTE, aplicativos de dados que não necessitam de priorização, como páginas WEB, e-mails. Para esta classe a rede deverá permitir

o fluxo do tráfego de dados por meio da técnica Best Effort e impedindo que esse tráfego afete negativamente as demais classes;

7.7. Caso os aplicativos já marquem os pacotes de dados, os equipamentos instalados deverão priorizá-los conforme programado. A rede da CONTRATADA deverá implementar a priorização através de alocação dinâmica de banda, dando preferência a pacotes marcados como Tempo Real e Dados Prioritários, respectivamente;

7.8. A banda a ser definida para cada classe de serviço em cada acesso da rede será acordada futuramente entre o CONTRATANTE e a CONTRATADA, quando da solicitação do serviço;

7.9. O serviço contratado deverá permitir modificações ou ampliações sem que estas impliquem na interrupção do restante das conexões da rede;

7.10. Poderão ser solicitados, durante a vigência do contrato, novos acessos, alterações de velocidade, de tipo, de classes de serviços ou mudanças de endereço;

7.11. Quaisquer alterações dos serviços serão solicitadas pelo CONTRATANTE, através de documento próprio a ser definido após a assinatura do contrato;

7.12. É de responsabilidade do CONTRATANTE definir o endereçamento IP da rede, bem como suas regras de roteamento;

7.13. Caso o CONTRATANTE necessite alterar o endereçamento IP e/ou as regras de roteamento, o prazo de atendimento será acordado entre as partes e a solicitação será mediante ofício entregue a CONTRATADA;

7.14. Parâmetros de Qualidade e Níveis de Serviço (SLA):

- Disponibilidade mínima mensal do serviço: 99,35%;
- Taxa de erros máxima admitida: 10^{-6};
- Latência média máxima da rede: 150 milissegundos;
- Para o Limiar de qualidade para perda de pacotes, deverá ser considerado menor ou igual a 2%;

7.15. Tempo máximo para mudança de velocidade de 30 (trinta) dias corridos a partir da data de solicitação, interrompendo o serviço por no máximo 1 (uma) hora;

7.16. Tempo máximo para mudança de endereço de 30 (trinta) dias corridos a partir da data de solicitação, mantendo o acesso antigo em funcionamento até 2 (duas) horas antes da ativação do novo acesso no novo endereço;

7.17. Prazo para recuperação/reparação do serviço (normalização do serviço após o registro da degradação, falha, defeito e/ou paralisação): no máximo 06 (seis) horas para todos os municípios.

Nota: A contagem dos prazos iniciar-se-á após a confirmação da abertura do chamado técnico. O procedimento será acordado entre o CONTRATANTE e a CONTRATADA.

7.18. A interface para entrega do serviço deverá ser 2 (duas) Portas Ethernet Full-Duplex (100/1000 Base-T) com conector RJ-45 fêmea. Todos os equipamentos, acessórios e recursos necessários (exceto energia elétrica), são de responsabilidade da CONTRATADA e deverão ser dimensionados para operar abaixo de sua capacidade nominal máxima;

8. DAS PENALIDADES

8.1. As penalidades abaixo serão aplicadas sobre os valores individuais de cada acesso analisado e constarão na fatura mensal do período subsequente ao da(s) ocorrência(s). No caso de descumprimento, pela CONTRATADA, de mais de um Nível de Serviço acordado, num mesmo período, num determinado acesso, as penalidades serão somadas até o valor máximo de 100% (cem por cento):

a) Taxa de erros média mensal (mínimo de dez amostras, em dias distintos) maior que a contratada: 10%;

b) Latência média mensal (mínimo de dez amostras, em dias distintos) maior que a contratada: 10%;

c) Prazo de instalação ou de mudança de endereço de instalação ou de mudança de velocidade maior que o contratado: 10% + 0,5% por dia inteiro de atraso;

d) Prazo para recuperação/reparação do serviço maior que o contratado: 10% + 1% por hora inteira de atraso;

e) Disponibilidade mensal medida do serviço:

- De 99,36% a 99%: 5%;
- De 98,9% a 98,5%: 10%;
- De 99,5% a 98,5%: 15%;
- De 98,6% a 97,0%: 20%;
- De 96,9% a 96,5%: 25%;
- De 96,4% a 96,0%: 30%;
- Abaixo de 96,0%: 50%;

Nota: As penalidades poderão ser reduzidas ou anuladas caso a CONTRATADA justifique as ocorrências e o CONTRATANTE aceite tais justificativas.

8.2. A contratação de Acessos à Intranet para serem instalados fora da Área de Tarifação Básica e que não estiverem previstos no Termo de Referência poderá ocorrer desde que de comum acordo entre a CONTRATADA e o CONTRATANTE. Tal premissa deve-se ao caráter especial desse tipo de atendimento e sem ela poderia ser inalcançável o custo total do contrato, o que impediria aos licitantes elaborarem suas propostas.

9. PLANO DE INSTALAÇÃO DOS ACESSOS

9.1. No início do contrato, para a implantação da rede, a CONTRATADA deverá apresentar ao CONTRATANTE um Cronograma de Instalação, Configuração e Ativação dos Serviços Contratados. Após a implantação da rede, os prazos a serem respeitados são os definidos neste instrumento.

9.2. O cronograma poderá ser revisado em comum acordo entre o CONTRATANTE e a CONTRATADA;

9.3. A rede deverá estar instalada e com todos os serviços especificados em operação em até 90 (noventa) dias;

9.4. Os serviços de Gerenciamento e Monitoração deverão estar operantes, conforme item 11, 90 (noventa) dias;

9.5. Os prazos deste item contam-se a partir da data da assinatura da Ordem de Serviço.

10. GERÊNCIA E MONITORAMENTO DOS SERVIÇOS CONTRATADOS

10.1. <u>GERÊNCIA DA REDE</u>

10.1.1. A CONTRATADA deverá prover um serviço de gerenciamento, a partir do seu próprio CGR – Centro de Gerência de Rede, que deverá apresentar pelo menos as seguintes características de atendimento:

- Regime de trabalho 24 x 7 x 365;
- Acesso por Discagem Direta Gratuita (DDG – 0800);
- Abertura de chamados para intervenções técnicas proativa e reativa;

10.1.2. Nas ocorrências detectadas pelo Sistema de Gerência de Falhas (SGF), os analistas entrarão em contato proativamente com o responsável da CONTRATANTE, fornecendo informações precisas sobre a

interrupção no serviço detectada;

10.1.3. Os analistas do CGR farão a abertura do chamado para acionamento da área técnica de forma que esta última possa intervir no caso e restabelecer o serviço nas condições contratadas.

10.2. MONITORAMENTO DOS SERVIÇOS

10.2.1. A CONTRATADA disponibilizará ao CONTRATANTE acesso às seguintes informações acerca dos acessos da rede:

10.2.2. Status instantâneo de cada acesso (ativo/inativo) e o tempo decorrido desde a última mudança de status. Deverá ser disponibilizada uma visão diagramática de toda a rede (topologia da rede com informações dos serviços contratados) num display instalado no CONTRATANTE ou por meio de uma página WEB disponível na Intranet e/ou Internet com acesso controlado por senha a ser disponibilizada pela CONTRATADA;

10.2.3. Ocupação da banda total do acesso e da banda disponibilizada para cada Classe de Serviço configurada para cada acesso por hora e minuto;

10.2.4. Taxa de erro ou perda de pacotes em cada acesso;

10.2.5. Ocupação do processador e da memória de cada roteador;

10.2.6. Valores Máximos, mínimos e médios de todos os acessos contratados.

10.2.7. Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:

- Enlace: designação, tecnologia e nível de serviço;
- Roteador CPE: fabricante e modelo, configuração lógica e configuração física (tipos de placas, interfaces, memória, slots, dentre outros);
- Endereçamento lógico: endereços IPs e máscaras;

10.2.8. Geração de relatórios consolidados com informação do histórico de chamados técnicos de cada acesso com a data e horário da abertura e do encerramento, tempo para a recuperação do serviço e causa da ocorrência.

10.2.9. A Solução de Gerenciamento e Monitoração da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados.

PARÁGRAFO SEGUNDO – RECEBIMENTO:

1. Os materiais serão recebidos pela Comissão de Recebimento de Materiais, formada por dois ou mais servidores do DER/RO, nomeados pelo Diretor Geral para tal finalidade, sendo que esta Comissão deverá seguir o estabelecido nos Artigos de 73 a 76 da Lei Federal Nº. 8.666/93.

2. O recebimento, conforme a Lei Federal nº 8.666/93 (Licitações e Contratos Administrativos) se dará na forma abaixo:

3. Serão os objetos deste Termo Contratual recebidos PROVISORIAMENTE, para efeito de verificação da conformidade em relação às especificações exigidas, no prazo máximo de 10 (dez) dias contados da data da efetiva entrega da Nota Fiscal/Fatura.

4. Serão os objetos deste Termo Contratual recebidos em DEFINITIVO no prazo máximo de dez (10) dias após a emissão do TERMO DE RECEBIMENTO PROVISÓRIO, que comprovará o recebimento em relação à qualidade e perfeita execução dos serviços, bem como, em relação à documentação necessária ao seu pagamento, conforme especificado neste Termo de Referência;

5. No recebimento DEFINITIVO dos serviços, quando houver dimensionamento do valor da Nota Fiscal ou Fatura em decorrência do resultado do Instrumento de Medição de Resultado, bem como no caso de glosa parcial dos serviços, a empresa deverá emitir Nota Fiscal ou Fatura com o valor exato, evitando, assim, efeitos tributários sobre valor não aceito pela Administração;

6. O recebimento provisório ou definitivo, não exclui a responsabilidade civil pela qualidade, correção, solidez e segurança do objeto contratual, nem ético profissional, pela perfeita execução do contrato;

PARÁGRAFO TERCEIRO - LOCAL DE UTILIZAÇÃO: Os locais a serem executados o objeto deste termo serão de acordo com o descriminado abaixo:

1ª RR DE COLORADO DO OESTE

RUA: ESTRADA DE SANTO ANTÔNIO N° 5323 – BAIRRO MILITAR, CEP: 78.916-610

RUA: AMAPÁ Nº 5329, BAIRRO: SÃO JOSÉ
CEP: 76.993-970

(69) 3341-2177

COLORADO DO OESTE / RO

3ª RR DE OURO PRETO D'OESTE

RUA: BURAREIRO S/Nº SETOR INDUSTRIAL
CEP: 76-920-000

(69) 3461-2549

OURO PRETO DO OESTE

4ª RR DE CACOAL

RUA: RONDÔNIA Nº 1078 BAIRRO: INCRA

CEP:76.965-872

(69) 3441-2621

CACOAL / RO

5ª RR DE ROLIM DE MOURA

AV: SETE DE SETEMBRO Nº 5490 BAIRRO: BOA ESPERANÇA
CEP: 76.940-000

(69) 3442-1619 3442-2321

ROLIM DE MOURA

6ª RR DE MACHADINHO D'OESTE
RO 133 Nº 4041

CEP: 76.868-000

(69)3581-3429

MACHADINHO DO OESTE

7ª RR DE ALVORADA D'OESTE
AV:INDEPENDENCIA S/Nº BAIRRO: ALTO ALEGRE
CEP: 76.930-000

(69)9.9286-1032 E 98469-3151
ALVORADA DO OESTE / RO

8ª RR DE JI-PARANÁ

BR 364 – KM 08 SETOR RURAL

CEP:76.900-000

(69) 3416-4822, 3423-8055 E 3416-4865

JÍ PARANÁ / RO

9ª RR DE VILHENA

AV: JÔ SATO 1280 BAIRRO: BELA VISTA

(69) 321-2901

VILHENA / RO

11ª RR DE PIMENTA BUENO

RUA: RUI BARBOSA Nº 250 BEIRA RIO
CEP: 76.970-970

(69) 3451-3405

PIMENTA BUENO / RO

12ª RR DE JARU

RUA TAPAJÓS Nº 3963 SETOR 02

CEP:76.890-000

(69) 3521-1553 E 99278-3962

JARU / RO

15ª RR DE BURITIS

AV AYRTON SENNA Nº 3766 SETOR INDUSTRIAL
CEP:76.880-000

(69) 3238-3690

16ª RR DE SÃO FRANCISCO

RUA DOM JOAONº3436 BAIRRO CIDADE BAIXA

(69) 3621-2399

SÃO FRANCISCO DO GUAPORÉ / RO

USINA DE JI-PARANÁ

AV: EDSON LIMA Nº 3835 BAIRRO: JORGE TEIXEIRA

(69) 3424-1059

JÍ-PARANÁ / RO

USINA DE ROLIM DE MOURA

AV:MORUMBI/ ESQUINA C/ PARNAIBA S/N

(69) 9.8424-8313

ROLIM DE MOURA / RO

USINA DE JARU

RO 463 (PÁTIO DA COOAJA) BAIRRO: ZONA RURAL

(69) 99282 3476

JARU / RO

PARÁGRAFO QUARTO - ASSISTÊNCIA TÉCNICA: A licitante interessada deverá assumir, mediante declaração, o compromisso de prestar a assistência técnica dentro dos prazos determinados no Edital e, caso sua sede empresarial não seja em Rondônia, a indicação expressa de sua representante (nome, cnpj, endereço, responsável, telefone, etc.) para atividade objeto deste Termo de Referência. Caso a licitante já possua assistência técnica no Estado de Rondônia, deverá constar na Proposta de Preços.

PARÁGRAFO QUINTO - DA GARANTIA: Os produtos ofertados deverão atender aos dispositivos da Lei nº 8.078/90 (Código de Defesa do Consumidor) e às demais legislações pertinentes.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

PARÁGRAFO PRIMEIRO: Realizar os pagamentos nos prazos e condições estabelecidos na **CLÁUSULA SEXTA** deste instrumento.

PARÁGRAFO SEGUNDO: Prestar informações indispensáveis a regular execução do contrato e os esclarecimentos que venham a ser solicitados pela Contratada.

PARÁGRAFO TERCEIRO: Prestar informações indispensáveis a regular execução do contrato e os esclarecimentos que venham a ser solicitados pela Contratada.

PARÁGRAFO QUARTO: Registrar os defeitos, as falhas e as imperfeições detectadas e comunicar à Contratada.

PARÁGRAFO QUINTO: Remeter à Contratada a expedição da Ordem de Fornecimento para que se efetue seu recebimento no prazo estipulado.

PARÁGRAFO SEXTO: Zelar pela preservação do equilíbrio econômico-financeiro do contrato.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CONTRATADA

PARÁGRAFO PRIMEIRO: Manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificações exigidas nos instrumentos convocatórios;

PARÁGRAFO SEGUNDO: Não utilizar de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do que dispõe o artigo 7º, inciso XXXIII da Constituição Federal.

PARÁGRAFO TERCEIRO: Responsabilizar-se pela fiel execução do objeto.

PARÁGRAFO QAURTO: Entregar o objeto de acordo com as especificações constantes na proposta de preços, no prazo e local indicados na mesma.

PARÁGRAFO QUINTO: Fazer acompanhar, quando da entrega do material, a respectiva nota fiscal, na qual deve haver referência ao processo e a respectiva nota de empenho da despesa, na qual deverá constar o objeto da presente contratação com seus valores correspondentes.

PARÁGRAFO SEXTO: Reparar, corrigir, remover ou substituir, às suas expensas, as partes do objeto desta licitação em que se verificar vícios, defeitos ou incorreções, no prazo máximo de 05 (cinco) dias úteis a contar da notificação para tal.

PARÁGRAFO SÉTIMO: Responsabilizar-se pelos encargos trabalhistas, previdenciários e comerciais, bem como pelos custos de frete e de tributos, resultantes da execução do contrato.

PARÁGRAFO OITAVO: Responder integralmente por perdas e danos que vier a causar ao DER ou a terceiros em razão de ação ou omissão dolosa ou culposa, sua ou dos seus prepostos, se for o caso, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

PARÁGRAFO NONO: Responder integralmente por perdas e danos que vier a causar ao DER/RO ou a terceiros em razão de ação ou omissão dolosa ou culposa, sua ou dos prepostos, se for o caso, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

PARÁGRAFO DÉCIMO: Realizar testes e corrigir defeitos nos materiais/bens, inclusive com a sua substituição quando necessário, sem ônus para a Contratante.

PARÁGRAFO DÉCIMO PRIMEIRO: Para tramitação da medição e pagamento das faturas serão exigidos os documentos e informações, conforme o que se segue:

a) Nota Fiscal;

b) Certidão negativa da Fazenda Estadual;

c) Certidão negativa da Receita Federal;

d) Certidão da Dívida Ativa da União;

e) Certidão negativa do INSS;

f) Certidão negativa municipal;

g) Certidão de Regularidade do FGTS;

h) Guia GPS INSS (original / autenticada);

i) Guia GFIP INSS (original / autenticada);

j) Certidão Negativa de Débitos Fiscais Trabalhistas – CNDT.

PARÁGRAFO DÉCIMO SEGUNDO: A Contratada deverá se responsabilizar pelos encargos trabalhistas, previdenciários, fiscais, comerciais e outros custos, resultantes da execução do contrato.

PARÁGRAFO DÉCIMO TERCEIRO: A Contratada deverá comparecer para assinatura do instrumento de contrato (ou equivalente) e para recebimento da Ordem de Fornecimento no prazo de 05 (cinco) dias, a contar de sua notificação para essas finalidades.

PARÁGRAFO DÉCIMO QUINTO: A Contratada possui obrigação de aceitar supressões até 25% (vinte e cinco por cento) propostos pela Contratante, conforme previsto no art. 65, § 1º, da Lei nº 8.666/93, ficando os acréscimos vedados conforme § 1°, art. 15, do Decreto Estadual n. 18.340/13 (*Redação do parágrafo dada pelo Decreto n. 24.082 de 22/07/2019*).

PARÁGRAFO DÉCIMO SEXTO: Realizar cadastro no sistema SEI, bem como manter suas informações atualizadas até o término de suas obrigações.

CLÁUSULA QUINTA – DOS PREÇOS E DOS CRÉDITOS ORÇAMENTÁRIOS

PARÁGRAFO PRIMEIRO: O valor do presente Contrato é de **R$ 314.199,48** (trezentos e quatorze mil cento e noventa e nove reais e quarenta e oito centavos), de acordo com os valores especificados na Proposta de preços e Planilhas de Preços.

PARÁGRAFO SEGUNDO: As despesas decorrentes da aquisição dos materiais/bens correrão por conta dos recursos consignados na Fonte de Recurso: **100**, Programa de atividade: 26.122.1015.2087, Elemento de Despesa: 33.90.40, do ano de 2021, provenientes do **DEPARTAMENTO ESTADUAL DE ESTRADAS DE RODAGEM E TRANSPORTES DER-RO**, e correndo à conta da seguinte programação:

R$ 130.916,45 (cento e trinta mil novecentos e dezesseis reais e quarenta e cinco centavos) , Programa / Atividade – 26.122.1015.2087 – Fonte: 0100– Elemento de Despesa 33.90.40, Dispensa de Licitação - Modalidade: Global, conforme Nota de Empenho nº 2021NE000941 de 11.08.2021 (0019916751).

O valor remanescente correrá à conta dos recursos orçamentários assegurados e será empenhado no decorrer do exercício de 2022, conforme Declaração de Adequação Financeira (0018818033).

CLÁUSULA SEXTA – DO PAGAMENTO

1. O pagamento será realizado por meio de ordem bancária e depósito em conta bancária informada pela Contratada, no prazo de até 30 (trinta) dias, contados da entrega, mediante apresentação da Nota Fiscal/Fatura devidamente certificada pela Comissão de Recebimento, sendo efetuada a retenção na fonte dos tributos e contribuições elencadas nas disposições determinadas pelos órgão fiscais e fazendários, em conformidade com as legislações e instruções normativas vigentes;

2. As notas fiscais/faturas deverão ser emitidas em 02 (duas) vias e apresentadas à Contratante para certificação, devendo conter em seu corpo a descrição do objeto, a indicação do número do contrato e da conta bancária da Contratada.

3. A(s) Nota(s) Fiscal(is)/Fatura(s) deverá(ão), ainda, estar acompanhada(s), obrigatoriamente, das certidões que atestem a regularidade perante as Fazendas Federal, Estadual e Municipal, ao recolhimento do FGTS e do INSS e aos Débitos Trabalhistas.

4. Em caso de atraso de pagamento, motivado exclusivamente pela Administração Contratante, o valor devido deverá ser acrescido de atualização monetária, a ser calculada entre a data limite para o pagamento e o efetivo adimplemento da parcela, mediante a aplicação da seguinte fórmula:

EM = N x VP x I, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da Parcela a ser paga

I = Índice de compensação financeira, assim apurado:

I = (TX/100)/365 I = ...

TX = Percentual atribuído ao Índice Nacional de Preços ao Consumidor Amplo - IPCA.

5. Havendo erro ou irregularidade na Nota Fiscal/Fatura ou circunstância que impeça a liquidação da despesa, aquela será devolvida à Contratada para as necessárias correções, com as informações que motivam sua rejeição, e o pagamento ficará pendente até que se providenciem as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou apresentação de novo documento fiscal não acarretando qualquer ônus para a Contratante.

6. A Administração não pagará, sem que tenha autorização prévia e formalmente, nenhum compromisso que lhe venha a ser cobrado diretamente por terceiros, sejam ou não instituições financeiras, à exceção de determinações judiciais, devidamente protocoladas no órgão.

12. Os eventuais encargos financeiros, processuais e outros, decorrentes da inobservância, pela contratada, de prazo de pagamento, serão de sua exclusiva responsabilidade.

CLÁUSULA SÉTIMA - DA VIGÊNCIA:

PARÁGRAFO PRIMEIRO: O Contrato terá vigência de 12 (doze) meses a contar da data de sua assinatura.

PARÁGRAFO SEGUNDO: A Contratante poderá modificar unilateralmente o contrato para melhor adequá-lo às finalidades de interesse de qualquer dos órgãos beneficiados pela contratação, respeitados os direitos da Contratada, conforme o art. 58, inciso I e o art. 65, inciso I todos da Lei Nº. 8.666/93;

CLÁUSULA OITAVA – DAS SANÇÕES:

PARÁGRAFO PRIMEIRO: Pela Inexecução total ou parcial do objeto, o DER-RO poderá, garantida a prévia defesa, aplicar à empresa contratada as seguintes sanções:

1.1. Advertência, que será aplicada por meio de notificação, estabelecendo o prazo de 05 (cinco) dias úteis para que a empresa contratada apresente justificativas para o atraso, que só serão aceitas mediante crivo da Administração;

2. Multa moratória correspondente a 0,5% (cinco décimos por cento) sobre o valor do contrato, por dia de atraso no cumprimento das obrigações assumidas, até a data do efetivo adimplemento, observado o limite de 10 (dez) dias corridos, após o qual será caracterizada a inexecução parcial ou total do contrato, conforme o caso;

2.1. A multa moratória será aplicada a partir do 1º dia útil da inadimplência, contado da data definida para o regular cumprimento da obrigação;

3. Multa moratória de 0,5% (cinco décimos por cento) sobre o valor do contrato, por dia de atraso na assinatura do instrumento contratual ou no recebimento da Ordem de Fornecimento ou da Nota de

Emprenho, observado o limite de 10 (dez) dias corridos, após o qual será caracterizada a inexecução total do contrato, salvo no caso de justificativa aceita pela Administração;

4. Multa de 10% (dez por cento) sobre o valor do contrato, pela recusa injustificada em assinar o contrato, em aceitar ou retirar o instrumento equivalente (nota de empenho), ou em receber a Ordem de Fornecimento, caso em que será caracterizada a inexecução total do contrato, salvo no caso de justificativa aceita pela Administração;

5. Multa de 10% (dez por cento) sobre o valor do produto não entregue, no caso de inexecução parcial, sem embargo de indenização dos prejuízos porventura causados ao DER/RO pela execução parcial do contrato;

6. Multa de 10% (dez por cento) sobre o valor total do contrato, no caso de sua inexecução total, sem embargo de indenização dos prejuízos porventura causados ao DER/RO;

7. Multa de 10% (dez por cento) sobre o valor do produto não entregue, pela recusa injustificada na substituição de material defeituoso no prazo estabelecido neste Termo de Referência;

8. Multa moratória de 0,5% (cinco décimos por cento) sobre o valor do produto não entregue, por dia de atraso na substituição do material defeituoso, observado o limite de 10 (dez) dias corridos, após o qual será considerada a inexecução parcial do contrato, salvo em caso de justificativa aceita pela administração;

PARÁGRAFO SEGUNDO: A multa prevista nos subitens **2, 3 e 8** poderão ser aplicadas isoladas ou em conjunto com as previstas nos subitens **5** e **6.**

PARÁGRAFO TERCEIRO: As multas eventualmente impostas à Contratada serão descontadas dos pagamentos a que fizer jus, acrescidas de juros moratórios de 1% (um por cento) ao mês. Caso a Contratada não tenha nenhum valor a receber do Contratante, ser-lhe-á concedido o prazo de 15 (quinze) dias corridos, contados de sua intimação, para efetuar o pagamento. Após esse prazo, não sendo efetuado o pagamento, os dados da Contratada serão encaminhados ao órgão competente para inscrição em dívida ativa.

PARÁGRAFO QUARTO: As penalidades serão obrigatoriamente registradas no cadastro estadual de fornecedores impedidos de licitar, e no caso de suspensão de licitar, a empresa contratada deverá ser descredenciada por igual período, sem prejuízo das multas previstas das demais cominações legais.

CLÁUSULA NONA – DA RESCISÃO

PARÁGRAFO PRIMEIRO: O descumprimento de qualquer Cláusula ou de simples condição deste Contrato, assim como a execução do seu objeto em desacordo com o estabelecido em suas Cláusulas e Condições, dará direito à **CONTRATANTE** de rescindi-lo mediante notificação expressa, sem que caiba à **CONTRATADA** qualquer direito, exceto o de receber o estrito valor correspondente ao fornecimento realizado, desde que estejam de acordo com as prescrições ora pactuadas, assegurada a defesa prévia.

PARÁGRAFO SEGUNDO: O contrato poderá rescindir a qualquer tempo, mediante decisão judicial ou denúncia escrita entre as partes, com antecedência mínima de 90 (noventa) dias, ocorrendo quaisquer das situações prevista no Art. 78, da Lei 8.666/93, ou ainda pela inobservância de quaisquer condições pactuadas no instrumento contratual.

PARÁGRAFO TERCEIRO: Este Contrato poderá, ainda, ser rescindido nos seguintes casos:

1. Decretação de falência, pedido de concordata ou dissolução da **CONTRATADA**;
2. Alteração do Contrato Social ou a modificação da finalidade ou da estrutura da **CONTRATADA**, que, a juízo da **CONTRATANTE**, prejudique a execução deste pacto;
3. Transferência dos direitos e/ou obrigações pertinentes a este Contrato, sem prévia e expressa autorização da **CONTRATANTE**;
4. Cometimento reiterado de faltas, devidamente anotadas;

5. No interesse da **CONTRATANTE**, mediante comunicação com antecedência de 05 (cinco) dias corridos, com o pagamento dos materiais/bens adquiridos até a data comunicada no aviso de rescisão;
5. No caso de descumprimento da legislação sobre trabalho de menores, nos termos do disposto no inciso XXXIII do Art. 7º da Constituição Federal.

CLÁUSULA DÉCIMA – DA PUBLICAÇÃO

PARÁGRAFO ÚNICO: A publicação do presente Contrato no Diário Oficial, por extrato, será providenciada até o 5° (quinto) dia útil do mês seguinte ao de sua assinatura, para ocorrer no **prazo de 20 (vinte) dias corridos,** daquela data, correndo as despesas às expensas da **CONTRATANTE**.

CLÁUSULA DÉCIMA PRIMEIRA – DA SUBCONTRATAÇÃO

PARÁGRAFO ÚNICO: Ficam vedadas a subcontratação total ou parcial do objeto, e a cessão ou transferência total ou parcial de quaisquer direitos e/ou obrigações inerentes ao presente contrato, por parte da CONTRATADA.

CLÁUSULA DÉCIMA SEGUNDA – DA FRAUDE E DA CORRUPÇÃO

PARÁGRAFO ÚNICO: A **CONTRATADA** deverá observar os mais altos padrões éticos durante a execução do Contrato, estando sujeitas às sanções previstas na legislação em caso de inobservância.

CLÁUSULA DÉCIMA TERCEIRO – DAS DISPOSIÇÕES FINAIS

PARÁGRAFO PRIMEIRO: Declaram as partes que este Contrato corresponde à manifestação final, completa e exclusiva do acordo entre elas celebrado.

PARÁGRAFO SEGUNDO: O reconhecimento dos direitos da Administração, em caso de rescisão administrativa prevista no art. 77 da Lei 8.666/93;

PARÁGRAFO TERCEIRO: A rescisão administrativa do contrato em razão da inexecução total ou parcial do seu objeto, sem prejuízo das sanções previstas na Cláusula Oitava, acarreta as seguintes consequências:

1. Assunção imediata do objeto do contrato, no estado e local em que se encontrar, por ato próprio da administração;
2. Ocupação e utilização do local, instalações, equipamentos, material e pessoal empregados na execução do contrato, necessários a sua continuidade na forma do inciso V do artigo 58 da Lei 8.666/93;
3. Execução da garantia contratual, caso prestada, para ressarcimento da Administração, e dos valores das multas e indenizações a elas devidas;
4. Retenção dos créditos decorrentes do contrato até o limite dos prejuízos causados à Administração.

PARÁGRAFO QUARTO: Ficam os termos do presente contrato vinculados às regras definidas nos instrumentos convocatórios integrantes neste procedimento.

CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS

PARÁGRAFO ÚNICO: Fica estabelecido, caso venha ocorrer algum fato não previsto neste termo de referência e seus anexos, os chamados casos omissos, que estes serão dirimidos respeitando o objeto dessa licitação, por meio de aplicação da legislação e demais normas reguladoras da matéria, em especial a lei n°8.666/93 e 10.520/02, aplicando-se paralelamente, quando for o caso, supletivamente, os

princípios da teoria geral dos contratos estabelecidos na legislação civil brasileira e as disposições de direito privado.

CLÁUSULA DÉCIMA QUINTA – PRAZO PARA ASSINATURA DO CONTATO:

PARÁGRAFO ÚNICO: Será de 05 (cinco) dias a contar do recebimento da convocação, através da disponibilização através do sistema sei.

CLÁUSULA DÉCIMA SEXTA – DO FORO

PARÁGRAFO PRIMEIRO: Fica eleito pelas partes o Foro da Comarca de Porto Velho, Capital do Estado de Rondônia, para dirimir todas e quaisquer questões oriundas do presente ajuste, inclusive às questões entre a empresa **CONTRATADA** e a **CONTRATANTE,** decorrentes da execução deste **CONTRATO**, com renúncia expressa de qualquer outro, por mais privilegiado que seja**.**

PARÁGRAFO SEGUNDO: Para firmeza e como prova do acordado, é lavrado o presente **TERMO DE CONTRATO,** segundo as informações e documentos constantes dos autos do processo identificado neste instrumento, o qual, depois de lido e achado conforme, vai assinado eletronicamente pelas partes, com a sua posterior publicação no Diário Oficial do Estado, nos termos do que dispõe o art. 61, Parágrafo Único da Lei nº 8.666/93.

Porto Velho/RO, 19 de agosto de 2021.

ELIAS REZENDE DE OLIVEIRA
Diretor Geral do DER/RO

JULIANO MURILO COCO
NBS SERVICOS DE COMUNICACOES LTDA

Visto pelo Procurador do DER-RO.

Documento assinado eletronicamente por **JULIANO MURILO COCO**, **Usuário Externo**, em 23/08/2021, às 11:22, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **ELIAS REZENDE DE OLIVEIRA**, **Diretor(a)**, em 31/08/2021, às 16:24, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Reinaldo Roberto dos Santos**, **Procurador(a)**, em 01/09/2021, às 09:37, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0020024514** e o código CRC **61C5D1CC**.