



CONTRATO DE PRESTAÇÃO DE SERVIÇOS EMERGENCIAL POR MEIO DE REDE PRIVADA DE COMUNICAÇÃO MULTISSERVIÇO (REDE WAN), QUE ENTRE SI FAZEM O BANCO DA AMAZÔNIA S.A. E A EMPRESA CLARO S.A.

Por este instrumento particular de Contrato, em que são Partes, de um lado o **BANCO DA AMAZÔNIA S.A.**, Sociedade de Economia Mista, vinculado ao Governo Federal, com sede em Belém (PA), situado na Avenida Presidente Vargas, nº 800, inscrito no CNPJ/MF sob o nº 04.902.979/0001-44, representado neste ato por sua Gerente Executiva da Gerência de Contratações e Gestão Administrativa de Contratos - GECOG, Sra. **BRUNA ELINE DA SILVA CAVALCANTE**, brasileira, solteira, bancária, portadora da Carteira de Identidade Profissional nº 25700 OAB/PA e CPF/MF 796.223.562-49 nesta cidade, doravante denominado **CONTRATANTE**, e de outro lado a empresa **CLARO S.A.**, sociedade anônima de capital fechado, com registro na Junta Comercial do Estado de São Paulo (JUCESP) sob o NIRE 35.300.145.801, com sede em São Paulo/SP, na Rua Henri Dunant, nº 780, Torres A e B, Bairro Santo Amaro, CEP: 04.709-110, inscrita no CNPJ/MF sob o nº 40.432.544/0001-47, representada neste ato por Procuração, pela sua Gerente Executiva de Contas, Sra. **LUCIANA COSTA CONCEIÇÃO**, brasileira, casada, gerente executiva de contas, portadora da Carteira de Identidade Profissional nº 14580D CRE/PA e do CPF/MF nº 802.396.502-63, doravante denominada **CONTRATADA**, por este instrumento e na melhor forma de direito, nos termos da decisão do Comitê de Governança das Aquisições-COGA do **CONTRATANTE**, datada de 11/12/2025, observado processo de contratação "**Emergencial**" e com base na proposta datada de 31/10/2025 da **CONTRATADA**, ajustam o presente Contrato nos termos do Art. 29, Inciso XV, da Lei 13.303/2016, sujeitando, ainda, as partes às demais disposições da Lei nº 13.303/2016 e às normas do Direito Privado, firmam o presente Contrato conforme Cláusulas a seguir.

DO OBJETO

CLÁUSULA PRIMEIRA – Contratação de empresa especializada em caráter "**emergencial**", cujo o objeto é a prestação de serviços de Comunicação por meio de **Rede Privada de Comunicação Multisserviço MPLS** com enlaces de transmissão, hardware, software para a interligação corporativa das redes locais (LAN) e Metropolitanas (MAN), abrangendo a Direção Geral, Superintendências, Agências, Postos Bancários e rede parceiros, com **Balanceamento Seguro de circuitos** e **Solução WIFI**, incluindo **Sistema de Gerenciamento e Monitoração WAN** e fornecimento de **Acessos a rede Internet** com proteção **Anti-DDoS Volumétrico**, **Anti-DDoS Camada de Aplicação**, **Segurança e proteção da rede LAN (NGFW)** e **Rede Dedicada de Alta Velocidade**.

PARÁGRAFO PRIMEIRO - Este Contrato deverá considerar os Lotes definidos abaixo, a saber:

LOTE	Descrição
01	Rede privada de comunicação multisserviço mpls com enlaces de transmissão, hardware, software para a interligação corporativa das redes locais (LAN) e metropolitanas (MAN), abrangendo a direção geral, superintendências, agências, postos bancários e rede parceiros, com balanceamento seguro de circuitos, fornecimento de solução WIFI, incluindo sistema de gerenciamento e monitoração WAN.



02	Prestação de serviços de rede de alta velocidade (LAN-TO-LAN) , através de circuitos de alta velocidade para contingência e replicação do banco de dados entre os Datacenters primário e secundário da contratante, utilizando acessos de fibra óptica em anel e interfaces giga ethernet (GE) a serem prontamente utilizados em caso de desastre/falhas no site principal
03	Acessos a rede internet nos datacenters do CONTRATANTE com fornecimento de serviço de proteção anti-ddos volumétrico, anti-ddos camada de aplicação, segurança e proteção da rede lan (NGFW). (Operadora 01).

PARÁGRAFO SEGUNDO - A proposta comercial apresentada pela **CONTRATADA**, datada de 31/10/2025, fica fazendo parte integrante deste Contrato como se nele estivesse transcrita

DO PRAZO DE EXECUÇÃO/ENTREGA DO OBJETO DA CONTRATAÇÃO

CLÁUSULA SEGUNDA - O prazo para implantação dos serviços nas Capitais dos Estados e no Interior serão listados na tabela abaixo sendo que todos os prazos são firmados a contar da data de assinatura do Contrato:

LOTE 01		
ITEM	RECURSO	PRAZO IMPLANTAÇÃO
01	REDE PRIVADA DE COMUNICAÇÃO MULTISSERVIÇO MPLS;	A partir da Assinatura do Contrato
02	BALANCEAMENTO SEGURO DE CIRCUITOS;	A partir da Assinatura do Contrato
03	SOLUÇÃO WIFI;	A partir da Assinatura do Contrato
04	SISTEMA DE GERENCIAMENTO E MONITORAÇÃO WAN;	A partir da Assinatura do Contrato

LOTE 02 (Rede de Alta velocidade)	
RECURSO	PRAZO IMPLANTAÇÃO
REDE DE ALTA VELOCIDADE (LAN-TO-LAN)	A partir da Assinatura do Contrato

LOTE 03 (Operadora 01)	
RECURSO	PRAZO IMPLANTAÇÃO
ACESSOS A REDE INTERNET NOS DATACENTERS;	A partir da Assinatura do Contrato
ANTI-DDOS VOLUMÉTRICO	A partir da Assinatura do Contrato
ANTI-DDOS CAMADA DE APLICAÇÃO	A partir da Assinatura do contrato
SEGURANÇA E PROTEÇÃO DA REDE LAN (NGFW)	A partir da Assinatura do Contrato

PARÁGRAFO PRIMEIRO Todos os prazos da tabela acima são limites; serviços podem ser entregues antes, mas o descumprimento acarretará multas conforme este Contrato.

PARÁGRAFO SEGUNDO - Caso não seja possível o cumprimento do prazo estabelecido, a **CONTRATADA** deverá comunicar formalmente as razões com antecedência mínima de 10 (dez) dias corridos, sob pena de aplicação das penalidades previstas neste Contrato, ressalvadas situações de caso fortuito e força maior, devidamente justificadas e aceitas pela **CONTRATANTE**.



DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO E DAS ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

CLÁUSULA TERCEIRA - A solução contratada consiste na prestação de serviços técnicos especializados de telecomunicações para a implementação e operação de uma Rede Privada de Comunicação Multisserviço (MPLS), com cobertura nacional, suporte completo e gerenciamento centralizado, abrangendo as Unidades do **CONTRATANTE** distribuídas na Amazônia Legal.

PARÁGRAFO PRIMEIRO - A rede deverá possuir topologia lógica do tipo full-mesh, com conectividade redundante entre todos os pontos, balanceamento de carga inteligente, qualidade de serviço (QoS) fim a fim e mecanismos de alta disponibilidade (HA), inclusive entre os datacenters primário e secundário do **CONTRATANTE**.

PARÁGRAFO SEGUNDO - A arquitetura da solução incluirá os seguintes componentes:

- I. Rede IP/MPLS multisserviço: para interligação das redes locais (LAN) e metropolitanas (MAN), com suporte a múltiplas classes de serviço, priorização de tráfego sensível (voz, vídeo, transações bancárias) e protocolos BGP, HSRP, entre outros.
- II. Sistema de gerenciamento e monitoramento WAN: plataforma centralizada baseada em SaaS, com recursos de detecção proativa por inteligência artificial, visibilidade total da rede, exportação de dados (NetFlow/sFlow), alarmes SNMP/syslog e dashboards operacionais.
- III. Infraestrutura Wi-Fi corporativa: fornecimento e gestão de access points com tecnologia 802.11ac Wave 2, controle de banda por SSID e aplicação, autenticação segura, controle de acesso e gestão por perfil de usuário, com controladora em nuvem.
- IV. Equipamentos de borda (CPEs): roteadores com suporte a múltiplos links WAN, balanceamento, firewall stateful, IPS/IDS, VPN IPsec, segmentação de tráfego e filtros de conteúdo.
- V. Acessos dedicados à Internet com proteção anti-DDoS: múltiplos pontos de saída em fibra óptica redundante, com mitigação de ataques volumétricos e de aplicação, roteamento BGP e solução NGFW com inspeção SSL.
- VI. Rede dedicada de alta velocidade (LAN-to-LAN): links de 10 Gbps para interligação dos datacenters do **CONTRATANTE**, com suporte a replicação síncrona e contingência em caso de desastre, com interfaces Ethernet.
- VII. Rede parceiros: implementar a rede MPLS com suporte a MULTI-VRF para atender à comunicação com parceiros externos, permitindo à contratante realizar transações comerciais com sua rede de parceiros e clientes de forma segura e eficiente.

PARÁGRAFO TERCEIRO - Todos os serviços deverão ser prestados de forma contínua, em regime 24x7x365, com suporte técnico local nas Cidades de Belém/PA, Marabá/PA e Santarém/PA, e central de atendimento remoto com canal 0800.

PARÁGRAFO QUARTO - A **CONTRATADA** será responsável por toda a operação fim a fim da solução, incluindo fornecimento, instalação, configuração, ativação, testes, suporte técnico, substituição de equipamentos, garantia, treinamento inicial e documentação técnica atualizada.

PARÁGRAFO QUINTO - As especificações técnicas detalhadas por lote, encontram-se descritas no **Anexo VI – Especificações Técnicas dos Serviços** deste Contrato.

DA DEDICAÇÃO EXCLUSIVA COM OU SEM MÃO DE OBRA

CLÁUSULA QUARTA - Esta contratação não possui dedicação exclusiva de mão de Obra.



DOS REQUISITOS DA CONTRATAÇÃO

CLÁUSULA QUINTA - Requisitos de Integração.

PARÁGRAFO PRIMEIRO - A solução deverá ser compatível com os sistemas, plataformas e protocolos atualmente utilizados pelo **CONTRATANTE**, observando os seguintes critérios:

- I. Suporte a protocolos IP/MPLS, BGP, OSPF, SNMP, QoS, IPv4/IPv6, entre outros em operação;
- II. Compatibilidade com sistemas de autenticação, gerenciamento de rede e segurança da informação do **CONTRATANTE**;
- III. Integração com ambientes de nuvem pública (AWS, Azure, Google Cloud) e infraestrutura legada;
- IV. Interoperabilidade com roteadores e equipamentos existentes do **CONTRATANTE**, majoritariamente da marca Cisco.

PARÁGRAFO SEGUNDO - Requisitos Funcionais.

PARÁGRAFO TERCEIRO - A solução contratada deverá prover:

- I. Comunicação de dados por meio de Rede IP/MPLS com topologia full-mesh entre as Unidades do **CONTRATANTE**;
- II. Acesso redundante à Internet com mitigação DDoS e firewall de borda;
- III. Conectividade segura com nuvens públicas e redes de parceiros via MPLS;
- IV. Plataforma de gerenciamento proativo baseada em SaaS com dashboards, alarmes, relatórios e IA;
- V. Wi-Fi corporativo gerenciado em nuvem com controle por SSID e aplicação;
- VI. Balanceamento automático de links com contingência e alta disponibilidade;
- VII. SLA (**Anexo VII**) deste Contrato, mínimo de 99,7% para sites centrais e 99,3% para unidades remotas;
- VIII. Circuitos LAN-to-LAN de alta velocidade para replicação de dados entre datacenters

PARÁGRAFO QUARTO - Requisitos Não Funcionais.

PARÁGRAFO QUINTO - A solução deverá atender aos seguintes atributos:

- I. Escalabilidade: Suporte a crescimento modular da rede, novos pontos e maior tráfego;
- II. Alta disponibilidade e desempenho, com contingência automática em caso de falha;
- III. Segurança lógica fim a fim com autenticação, criptografia, segregação de tráfego e controle de acesso;
- IV. Monitoramento e gestão centralizados, com logs e relatórios acessíveis ao **CONTRATANTE**;
- V. Compatibilidade com políticas de segurança e continuidade de negócios do **CONTRATANTE**

PARÁGRAFO SEXTO - Necessidade de Treinamentos e Requisitos para Implementação da Solução.

PARÁGRAFO SÉTIMO - A **CONTRATADA** deverá oferecer, sem ônus para ao **CONTRATANTE**:

- I. Treinamento técnico e prático (hands-on) com carga horária mínima de 40 horas por módulo;



- II. Conteúdo abrangendo gestão de rede, sd-wan, QoS, segurança, relatórios e contingência;
- III. Material didático digital e presencial, ministrado por profissionais certificados;
- IV. Suporte adicional pós-treinamento por 90 (noventa) dias;
- V. Demonstração funcional durante implantação;
- VI. Realização do treinamento em formato online ou nas dependências do **CONTRATANTE**.

PARÁGRAFO OITAVO - Indicação de Necessidade de Contratações Correlatas ou Interdependentes.

PARÁGRAFO NONO - A execução do objeto dependerá exclusivamente da **CONTRATADA**, sendo de sua responsabilidade:

- I. Fornecimento de todos os profissionais, equipamentos, insumos e ferramentas;
- II. Atendimento local e remoto (NOC 24x7x365), incluindo transporte e alimentação;
- III. Realização de configurações, integrações e homologações em conformidade com ao **CONTRATANTE**;
- IV. Fornecimento de manuais técnicos, EPI/EPC e equipamentos de suporte à execução dos serviços;
- V. Substituição de equipamentos com falha (RMA), conforme SLA estabelecido

PARÁGRAFO DÉCIMO - Requisitos de Segurança Adicionais.

PARÁGRAFO DÉCIMO PRIMEIRO - A solução deverá atender, adicionalmente, aos seguintes requisitos:

- I. Segmentação lógica de redes por tipo de serviço;
- II. Detecção e resposta a ameaças com base em padrões de tráfego e anomalias;
- III. Conformidade com requisitos do BACEN, LGPD e políticas internas do **CONTRATANTE**;
- IV. Armazenamento dos logs e métricas por no mínimo 12 (doze) meses, com acesso restrito e auditável.

PARÁGRAFO DÉCIMO SEGUNDO - Observações Específicas:

- I. Será admitida a padronização de equipamentos e serviços desde que tecnicamente justificada.
- II. Poderá ser exigido certificado de conformidade de fabricação e qualidade dos produtos utilizados.
- III. Não será permitida a contratação de um mesmo agente econômico para funções que exijam segregação, como fornecimento e fiscalização.
- IV. Excepcionalmente, poderá ser exigido modelo/marca específicos quando justificado pela compatibilidade com parque tecnológico existente, desempenho ou padronização operacional.

PARÁGRAFO DÉCIMO TERCEIRO - Integração com a Arquitetura de Redes do **CONTRATANTE**:

- I. A infraestrutura contratada deverá se integrar, de forma nativa, à Arquitetura de Redes Corporativas do **CONTRATANTE**, baseada em topologia lógica full-mesh e protocolos IP/MPLS, com suporte a QoS fim a fim, balanceamento de carga, contingência automática e roteamento dinâmico com suporte a BGP, OSPF, VRF e PBR.



II. Todos os componentes ativos de rede a serem fornecidos (roteadores CPE, switches, UTM, controladoras de acesso, sistemas de gerenciamento, etc.) deverão interoperar com os equipamentos existentes no backbone do **CONTRATANTE**, sem que haja degradação de desempenho, violação de política de segurança ou quebra de compatibilidade técnica.

III. A **CONTRATADA** deverá, ainda, garantir a correta integração dos enlaces físicos e lógicos à malha MPLS do **CONTRATANTE**, incluindo a configuração de túneis IPsec, tabelas de roteamento específicas, marcação de tráfego (DiffServ), definição de políticas de failover, acesso seguro à rede LAN e mecanismos de isolamento e redundância para os sites principais, secundários e unidades remotas, conforme descrito nas **Especificações Técnicas dos Serviços – Anexo VI** deste Contrato.

IV. Todas as configurações e integrações deverão respeitar as diretrizes internas do **CONTRATANTE** sobre segurança, segregação de redes, planos de endereçamento IP, autenticação, criptografia de dados, replicação entre datacenters e regras de acesso lógico entre as zonas de rede

PARÁGRAFO DÉCIMO QUARTO - Requisitos funcionais da solução:

I. A solução técnica a ser contratada deverá atender a todos os requisitos funcionais necessários à sustentação da operação da infraestrutura de comunicação de dados do **CONTRATANTE**, com vistas a garantir conectividade de alta disponibilidade, segurança cibernética, integração com ambientes críticos, flexibilidade operacional e aderência às diretrizes de modernização tecnológica da instituição.

PARÁGRAFO DÉCIMO QUINTO - Conectividade de Alta Performance para Projetos Estratégicos.

I. A solução deverá garantir a operação ininterrupta dos seguintes projetos e ambientes considerados estratégicos para o **CONTRATANTE**:

- a) Projeto de contingência e replicação de dados entre os datacenters principais, por meio de enlaces dedicados de alta velocidade (LAN-to-LAN);
- b) Comunicação via MPLS com parceiros comerciais, integradores de meios de pagamento, órgãos reguladores e redes de compensação;
- c) Provisão de conectividade robusta para os pontos de presença da rede institucional em áreas remotas da Amazônia Legal, com suporte a links redundantes e mecanismos de failover automático

PARÁGRAFO DÉCIMO SEXTO - Entregas Técnicas e Garantias de Atualização:

- I. Todos os elementos da solução, incluindo **roteadores CPE, controladoras Wi-Fi, UTM, NGFW, switches, ferramentas de gerenciamento e demais componentes de hardware e software**, deverão ser entregues em suas versões mais recentes, estáveis e homologadas pelo fabricante;
- II. Durante toda a vigência do contrato, a **CONTRATADA** deverá prover **atualizações contínuas de firmware, patches de segurança e upgrades de funcionalidades**, sem qualquer ônus adicional para o **CONTRATANTE**;
- III. Todos os produtos ofertados deverão apresentar **plena compatibilidade entre si**, e a solução deverá ser funcionalmente integrada, evitando ilhas tecnológicas;

PARÁGRAFO DÉCIMO SÉTIMO - Em caso de apontamento técnico de não conformidade por parte do **CONTRATANTE**, será assegurado à **CONTRATADA** o exercício do **contraditório e ampla defesa**, conforme normativos internos aplicáveis.

PARÁGRAFO DÉCIMO OITAVO - Indicação de Eventual Necessidade de Contratações Correlatas ou Interdependentes:



I. Considerando a natureza crítica da infraestrutura de comunicação de dados corporativa, bem como a abrangência geográfica do **CONTRATANTE**, **eventuais necessidades operacionais, técnicas ou logísticas** que impliquem em atividades adicionais para o correto funcionamento da solução contratada serão de inteira responsabilidade da **CONTRATADA**, sem quaisquer ônus adicionais para o **CONTRATANTE**.

II. Para garantir a operação estável e contínua da rede multiserviço, a **CONTRATADA** deverá prover, em caráter obrigatório, as seguintes condições

PARÁGRAFO DÉCIMO NONO - Alocação de Profissionais Qualificados:

I. A **CONTRATADA** deverá alocar, sempre que necessário, profissionais tecnicamente qualificados, com as respectivas certificações exigidas para os equipamentos e serviços contratados, incluindo todas as obrigações trabalhistas e previdenciárias decorrentes, em conformidade com a Legislação vigente.

II. Apoio Técnico e Logístico:

a) Deverá ser assegurado apoio técnico e logístico completo para o adequado funcionamento da solução, compreendendo o suporte às atividades de instalação, testes, manutenção corretiva e preventiva, substituições e atualizações dos elementos da infraestrutura.

III. Custos Operacionais e Logísticos:

a) Todos os custos necessários à execução dos serviços, incluindo, mas não se limitando a: **transporte, alimentação, hospedagem de profissionais, deslocamento de equipamentos, ligações telefônicas, abertura de chamados, montagem física, disponibilização de ferramentas e insumos**, fornecimento de projetos técnico serão integralmente absorvidos pela **CONTRATADA**.

IV. Configurações e Customizações para Alta Disponibilidade.

V. A **CONTRATADA** deverá realizar todas as **configurações e customizações necessárias** para assegurar a operação ininterrupta da solução, com mitigação proativa de falhas de desempenho, latência excessiva ou interrupções de serviço.

VI. Execução conforme Normas Técnicas e Fabricantes:

a) Todos os serviços deverão ser executados **em conformidade com as normas técnicas aplicáveis**, recomendações dos fabricantes, boas práticas de engenharia de redes e de segurança da informação, bem como com as orientações técnicas emitidas pelo **CONTRATANTE** durante a vigência contratual.

VII. Fornecimento de Ferramental e Documentação Técnica:

a) A **CONTRATADA** deverá fornecer a seus prepostos todo o ferramental necessário à execução dos serviços, inclusive **manuals técnicos, guias de instalação, operação e manutenção** dos equipamentos e sistemas, de forma a possibilitar pronta identificação de componentes e correta aplicação de procedimentos recomendados. Além disso, disponibilizar na assinatura do contrato um kit de ferramentas e testador de rede, para auxiliar nas instalações físicas e lógicas de equipamentos no Datacenter.

VIII. Equipamentos de Proteção:

a) Deverá ser assegurado o fornecimento de **Equipamentos de Proteção Individual (EPI) e Equipamentos de Proteção Coletiva (EPC)** a todos os profissionais da **CONTRATADA**, sempre que a natureza da atividade exigir, em especial em ambientes com acesso a instalações elétricas, infraestrutura predial ou manipulação física de equipamentos.

IX. Suporte Técnico 24x7:

a) A **CONTRATADA** deverá manter uma infraestrutura de suporte técnico operacional **em regime contínuo 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana**, incluindo finais de semana e feriados, de modo a atender prontamente quaisquer ocorrências relativas à prestação dos serviços.

**X. Suporte Técnico Remoto:**

a) Deverá ser disponibilizado suporte remoto (on-line) por meio de **canal telefônico, e-mail e sistema eletrônico de chamados (web-based)**, com atendimento por equipe técnica qualificada, apta a diagnosticar e solucionar incidentes de forma ágil e eficaz.

XI. Suporte Técnico Local:

a) Nos casos em que o atendimento remoto não for suficiente para restabelecer os serviços, a **CONTRATADA** deverá realizar **suporte técnico presencial (on-site)**, com envio de profissional capacitado até o(s) local(is) de instalação da solução, conforme as localidades contempladas no escopo da contratação, observando os prazos e níveis de serviço estabelecidos no **Acordo de Nível de Serviço (SLA) – Anexo VII** deste Contrato.

DOS REQUISITOS MÍNIMOS DE SEGURANÇA PARA SISTEMAS ADQUIRIDOS

CLÁUSULA SEXTA – Os requisitos mínimos de segurança para os sistemas adquiridos estão contidos no **Anexo V** deste Contrato.

DO PREÇO

CLÁUSULA SÉTIMA – Pelo fornecimento da solução e serviços ora contratados, o **CONTRATANTE** pagará à **CONTRATADA**, o Valor Mensal de **R\$753.191,91** (setecentos e cinquenta e três mil, cento e noventa e um reais e noventa e um centavos) e o Valor Global para 180 (cento e oitenta) dias de vigência contratual será de **R\$4.519.151,48** (quatro milhões, quinhentos e dezenove mil, cento e cinquenta e um reais e quarenta e oito centavos) de acordo com a **Proposta Comercial e Tabela – Anexo IX** deste Contrato, conforme abaixo:

Lote	Descrição	Mensal (R\$)	Anual (R\$)
01	REDE PRIVADA DE COMUNICAÇÃO MULTISSERVIÇO MPLS COM ENLACES DE TRANSMISSÃO, HARDWARE, SOFTWARE PARA A INTERLIGAÇÃO CORPORATIVA DAS REDES LOCAIS (LAN) E METROPOLITANAS (MAN), ABRANGENDO A DIREÇÃO GERAL, SUPERINTENDÊNCIAS, AGÊNCIAS, POSTOS BANCÁRIOS e REDE PARCEIROS, COM BALANCEAMENTO SEGURO DE CIRCUITOS, FORNECIMENTO DE SOLUÇÃO WIFI, INCLUINDO SISTEMA DE GERENCIAMENTO E MONITORAÇÃO WAN.	559.020,33	3.354.122,01
02	PRESTAÇÃO DE SERVIÇOS DE REDE DE ALTA VELOCIDADE (LAN-TO-LAN) . ATRAVÉS DE CIRCUITOS DE ALTA VELOCIDADE PARA CONTINGÊNCIA E REPLICAÇÃO DO BANCO DE DADOS ENTRE OS DATACENTERES PRIMÁRIO E SECUNDÁRIO DA CONTRATANTE, UTILIZANDO ACESSOS DE FIBRA ÓPTICA EM ANEL E INTERFACES GIGA ETHERNET (GE) A SEREM PRONTAMENTE UTILIZADOS EM CASO DE DESASTRE/FALHAS NO SITE PRINCIPAL	92.542,87	555.257,19

03	ACESSOS A REDE INTERNET NOS DATACENTERS DA CONTRATANTE COM FORNECIMENTO DE SERVIÇO DE PROTEÇÃO ANTI-DDOS VOLUMÉTRICO, ANTI-DDOS CAMADA DE APLICAÇÃO, SEGURANÇA E PROTEÇÃO DA REDE LAN (NGFW). (OPERADORA 01).	101.628,71	609.772,28
VALOR TOTAL GERAL		753.191,91	4.519.151,48

PARÁGRAFO ÚNICO - O preço indicado no *Caput* desta CLÁUSULA inclui todos os custos que incidem sobre a contratação:

DO PAGAMENTO

CLÁUSULA OITAVA - O pagamento será efetuado no prazo de até 30 (trinta) dias úteis, contados a partir da emissão do termo de recebimento definitivo, emitido pelo Fiscal do Contrato. O referido termo deve atestar o recebimento do serviço e/ou bem, o cumprimento do disposto nos itens abaixo, além de expressamente autorizar a emissão da nota fiscal, por meio de crédito na Conta Corrente de titularidade da **CONTRATADA**.

PARÁGRAFO PRIMEIRO - Notas Fiscais emitidas após o 25º do mês subsequente a prestação do serviço e/ou entrega do bem não serão aceitas pelo contratante, devendo a **CONTRATADA** emití-las a partir do 1º dia útil do mês seguinte.

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

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

PARÁGRAFO QUARTO - Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 30 (trinta) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

PARÁGRAFO QUINTO - Para fins de liquidação, o fiscal técnico deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- O prazo de validade;
- A data da emissão;
- Os dados do Contrato e do **CONTRATANTE**;
- O período respectivo de execução do Contrato.
- O valor a pagar; e eventual destaque do valor de retenções tributárias cabíveis.

PARÁGRAFO SEXTO - Caso a **CONTRATADA** opte pelo recebimento do pagamento em conta corrente mantida em outra instituição financeira, lhe será cobrado o valor da tarifa TED, correspondente ao da tabela de tarifas e serviços do banco, sendo que esse valor será de responsabilidade da **CONTRATADA** e deduzido do valor do crédito a ser enviado.



PARÁGRAFO SÉTIMO - Os pagamentos serão automaticamente transferidos para os dias úteis subsequentes, caso não haja expediente no banco nas datas previstas para tal.

PARÁGRAFO OITAVO - Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao **CONTRATANTE**.

PARÁGRAFO NONO - No caso de atraso pelo **CONTRATANTE**, os valores devidos a **CONTRATADA** serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA/IBGE de correção monetária.

PARÁGRAFO DÉCIMO - A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, social e trabalhista, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação estabelecida na contratação.

PARÁGRAFO DÉCIMO PRIMEIRO - O **CONTRATANTE** deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no Contrato; b) identificar possível razão que impeça a participação em licitação, no âmbito do Órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

PARÁGRAFO DÉCIMO SEGUNDO - Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada pelo Fiscal Técnico do Contrato a sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do **CONTRATANTE**.

PARÁGRAFO DÉCIMO TERCEIRO - Não havendo regularização ou sendo a defesa considerada improcedente, o **CONTRATANTE** deverá comunicar aos órgãos responsáveis pela Fiscalização da regularidade fiscal quanto à inadimplência da **CONTRATADA**, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

PARÁGRAFO DÉCIMO QUARTO - Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

PARÁGRAFO DÉCIMO QUINTO - Para efeito de pagamento, a **CONTRATADA** deverá apresentar juntamente com as notas fiscais/faturas discriminativas os documentos a seguir relacionados, caso não estejam disponíveis no Cadastro Único de Fornecedores (SICAF):

- a) Certidão negativa ou positiva com efeitos de negativa de débitos, conjunta, relativos aos tributos federais e à **Dívida Ativa da União** e INSS;
- b) Certidão negativa de débitos ou positiva com efeitos de negativa das Fazendas **Estadual e Municipal** de seu domicílio ou sede;
- c) Certidão de regularidade do **FGTS (CRF)**;
- d) Certidão Negativa de Débitos Trabalhistas – **CNDT**;
- e) Declaração do **Simples Nacional**, caso seja optante.



PARÁGRAFO DÉCIMO SEXTO - Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso a **CONTRATADA** não regularize sua situação junto ao SICAF.

DOS CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

CLÁUSULA NONA - Os serviços serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo (a) responsável pelo acompanhamento e Fiscalização do Contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Contrato e na proposta.

PARÁGRAFO PRIMEIRO - No ato de recebimento o Fiscal Técnico emitirá um Termo de Recebimento Provisório no prazo estipulado no item anterior.

PARÁGRAFO SEGUNDO - Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste Contrato e nas propostas comerciais, devendo ser substituídos no prazo de 10 (dez) dias úteis, a contar da notificação da **CONTRATADA**, às suas custas, sem prejuízo da aplicação das penalidades.

PARÁGRAFO TERCEIRO - O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

PARÁGRAFO QUARTO - No ato de recebimento o Fiscal Técnico emitirá um Termo de Recebimento Definitivo no prazo estipulado no Parágrafo anterior.

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

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

PARÁGRAFO SÉTIMO - O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do Contrato.

DO ORÇAMENTO

DAS RUBRICAS ORÇAMENTÁRIAS

CLÁUSULA DÉCIMA - Os recursos para dar cobertura a presente contratação estão previstos no orçamento do **CONTRATANTE** na Rubrica: **"81.225-0 Transmissão de dados."**

DA REPACTUAÇÃO DOS PREÇOS

CLÁUSULA DÉCIMA PRIMEIRA - Os preços contratados permanecerão fixos e irrevogáveis pelo prazo de vigência do Contrato.



DAS OBRIGAÇÕES DA CONTRATADA

CLÁUSULA DÉCIMA SEGUNDA - Constituem obrigações da **CONTRATADA**:

- I) A **CONTRATADA** obriga-se a cumprir integralmente as disposições previstas neste Termo de referência, no contrato e em seus anexos, observando as seguintes obrigações, sem prejuízo de outras que sejam inerentes ao cumprimento do objeto da contratação;
- II) **Obrigações Gerais:** Executar o objeto do contrato em conformidade com todas as especificações técnicas, prazos, níveis de serviço (SLA) e demais condições estabelecidas neste Contrato demais anexos que compõem o instrumento contratual
- III) Obedecer rigorosamente a todos os prazos estipulados para implantação, ativação, manutenção, suporte e correções, conforme cronograma e marcos contratuais definidos pelo **CONTRATANTE**.
- IV) Prestar, sempre que solicitado, esclarecimentos técnicos e administrativos sobre a execução do Contrato, bem como atender de forma tempestiva a eventuais **reclamações, notificações ou recomendações** emitidas pela fiscalização ou gestão contratual.
- V) Submeter-se à **fiscalização técnica e administrativa** do **CONTRATANTE**, facultando livre acesso a todas as instalações, sistemas, equipamentos, registros e documentos relacionados à execução do objeto.
- VI) Prover todos os **meios técnicos, humanos, materiais, logísticos e operacionais necessários à plena operacionalidade da Rede Multisserviço WAN**, incluindo hardware, software, enlaces de comunicação, mão de obra técnica e ferramentas de gerenciamento e segurança;
- VII) Manter absoluto sigilo e confidencialidade sobre **dados, documentos, topologias de rede, configurações, acessos, informações técnicas e estratégicas** do **CONTRATANTE**, aplicando medidas de proteção física e lógica conforme a legislação vigente (inclusive LGPD) e normas internas do **CONTRATANTE**;
- VIII) Exercer todas as atividades em **estrita conformidade com a legislação brasileira**, especialmente a Lei nº 13.303/2016, a Legislação de telecomunicações (ANATEL), leis ambientais, trabalhistas, fiscais, de segurança da informação e proteção de dados pessoais.
- IX) Não se utilizar, direta ou indiretamente, de trabalho ilegal, infantil ou análogo à escravidão, bem como garantir que todos os seus fornecedores, subcontratados e prestadores de serviço observem integralmente a legislação trabalhista.
- X) Adotar políticas e práticas que assegurem a **não discriminação** de qualquer natureza no ambiente de trabalho, em especial por motivo de raça, gênero, orientação sexual, idade, religião, condição física ou social.
- XI) Executar os serviços com **responsabilidade socioambiental**, observando integralmente a legislação ambiental vigente, com especial atenção ao descarte correto de materiais, à redução de resíduos eletrônicos e à prevenção de danos ao meio ambiente.
- XII) Corrigir imediatamente, sem ônus para o **CONTRATANTE**, quaisquer **falhas, deficiências, inconsistências ou desvios técnicos** identificados pela fiscalização durante a vigência contratual, dentro dos prazos estabelecidos em notificação formal..



XIII) Responder, na forma da lei, **pelos danos causados ao CONTRATANTE ou a terceiros**, inclusive aos bens patrimoniais do Banco ou de seus clientes, em decorrência de **ações ou omissões de seus empregados, subordinados ou prepostos**, desde que comprovada culpa ou dolo.

PARÁGRAFO ÚNICO - Obrigações Específicas Relacionadas à Rede WAN:

- I.** Garantir a alta disponibilidade da infraestrutura contratada, conforme **Acordo de Nível de Serviço (SLA) – Anexo VII** deste Contrato, com suporte técnico proativo 24x7x365, canais de atendimento eficazes e prazos de resposta e resolução compatíveis com a criticidade dos serviços.
- II.** Monitorar continuamente o desempenho e a integridade da rede, com uso de ferramentas de gerenciamento e inteligência artificial, fornecendo relatórios periódicos, indicadores de **Acordo de Nível de Serviço (SLA) – Anexo VII** deste Contrato e notificações em tempo real de eventos críticos.
- III.** Assegurar a contingência automática de enlaces, incluindo links principais e backup, e manter rotas alternativas ativas em conformidade com os protocolos e políticas de roteamento adotadas pelo **CONTRATANTE** (como BGP, VRF, QoS).
- IV.** Disponibilizar profissionais qualificados e certificados para todas as atividades de instalação, suporte, configuração e manutenção de equipamentos e serviços, conforme perfis mínimos estabelecidos neste Contrato.
- V.** Garantir a compatibilidade plena entre os equipamentos e sistemas ofertados, com atualizações regulares de firmware, patches de segurança e suporte técnico contínuo, sem interrupções nas operações do **CONTRATANTE**.
- VI.** Manter infraestrutura técnica e logística suficiente para atuação local ou regional, conforme exigência dos lotes, com capacidade de atendimento em áreas de difícil acesso, inclusive na Amazônia Legal.

DAS OBRIGAÇÕES DO CONTRATANTE

CLÁUSULA DÉCIMA TERCEIRA – Constituem obrigações do CONTRATANTE:

- I)** Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com as Cláusulas contratuais e os termos de sua proposta.
- II)** Designar formalmente os fiscais técnico e administrativo do contrato, os quais exercerão as atividades de acompanhamento e fiscalização da execução dos serviços, conforme previsto no Art. 117 da Lei nº 13.303/2016 e no Art. 99 do Regulamento de Licitações e Contratos do **CONTRATANTE**.
- III)** Atuar no controle e validação das entregas contratuais, por meio do atesto técnico das Notas Fiscais/Faturas correspondentes às etapas executadas, condicionando o pagamento à comprovação da conformidade dos serviços e ao cumprimento dos **Acordo de Nível de Serviço (SLA) – Anexo VII** deste Contrato, acordados.
- IV)** Exercer a Fiscalização dos serviços por empregados especialmente designados, na forma prevista na Lei nº 13.303/2016 e Art. 99 do Regulamento do **CONTRATANTE**.
- V)** Atestar através do Fiscal Técnico do Contrato as Notas Fiscais/ Fatura de Serviços correspondentes às etapas executadas, após a verificação da conformidade dos serviços, para efeito de pagamento.
- VI)** Rejeitar, total ou parcialmente, os serviços prestados em desacordo com as especificações técnicas, padrões de qualidade, cronograma, prazos ou qualquer outra obrigação prevista contratualmente, comunicando formalmente à **CONTRATADA** as não conformidades apuradas.



- VII)** Efetuar o pagamento das Notas Fiscais/Faturas apresentadas pela **CONTRATADA**, desde que protocoladas com antecedência mínima de 30 (trinta) dias do vencimento, e que os serviços prestados estejam integralmente atestados pelo setor técnico competente.
- VIII)** Promover a infraestrutura necessária à prestação dos serviços, incluindo instalações sanitárias, vestiários com armários guarda-roupas, local para guarda dos materiais, equipamentos, ferramentas e utensílios e outras que se apresentarem necessárias.
- IX)** Receber e identificar os prepostos da **CONTRATADA**, adotando as providências administrativas necessárias para garantir o acesso autorizado às dependências do **CONTRATANTE**, conforme normas de segurança institucional.
- X)** Disponibilizar os meios e recursos mínimos necessários à prestação dos serviços contratados, quando aplicável, incluindo:
- a. Acesso remoto (VPN) para diagnóstico e suporte;
 - b. Apoio logístico local, mediante solicitação prévia, nas unidades operacionais do **CONTRATANTE**;
 - c. Autorização para entrada em ambientes de missão crítica, mediante credenciamento prévio do(s) técnico(s) da **CONTRATADA**
- XI)** Assegurar que ordens e solicitações relativas à execução dos serviços sejam formalmente encaminhadas ao preposto da **CONTRATADA**, evitando interferência direta nos seus empregados, exceto em situações de emergência ou risco iminente.
- XII)** Notificar a **CONTRATADA**, por escrito, sempre que houver constatação de falhas, irregularidades ou infrações contratuais, estabelecendo prazo razoável para a sua correção, bem como aplicar penalidades administrativas, quando cabíveis, observando o contraditório e a ampla defesa.
- XIII)** Obrigações Complementares Específicas ao Objeto:
- a. Disponibilizar, quando necessário, as informações técnicas e operacionais essenciais para viabilizar a correta configuração dos equipamentos e enlaces contratados, sem que isso implique compartilhamento de informações sigilosas ou estratégicas.
 - b. Garantir a interlocução institucional com os demais setores do **CONTRATANTE** (como infraestrutura predial, segurança da informação, TI, logística e agências), para assegurar ambiente técnico e organizacional adequado à implantação e operação da solução WAN.
 - c. Planejar, com a devida antecedência, os procedimentos necessários à renovação, substituição ou nova contratação dos serviços, de forma a evitar descontinuidade na prestação dos serviços de conectividade ao término da vigência contratual.

DA HABILITAÇÃO

CLÁUSULA DÉCIMA QUARTA - A CONTRATADA também se obriga a manter, durante a vigência deste Contrato, todas as condições de habilitação exigidas na contratação. Assume, ainda, a obrigação de apresentar, no término do prazo de validade de cada documento, os seguintes comprovantes atualizados:

- a) Os comprovantes de regularidade de situação junto às Fazendas: **Estadual e Municipal** de seu domicílio ou sede;
- b) A certidão emitida pela Receita Federal negativa ou positiva com efeitos de negativa de débitos relativos aos tributos federais, inclusive as contribuições previdenciárias, e à **dívida ativa da União**;



c) O certificado de regularidade perante o **FGTS** - Fundo de Garantia do Tempo de Serviço, mediante apresentação do CRF - Certificado de Regularidade de Fundo de Garantia;

d) A certidão negativa ou positiva com efeitos de negativa de débitos trabalhistas (**CNDT**).

PARÁGRAFO ÚNICO - A não apresentação dos comprovantes citados acima poderá ensejar, a critério do **CONTRATANTE**, exceto quando os comprovantes estiverem disponíveis no Cadastro Único de Fornecedores (SICAF), a rescisão do Contrato a ser assinado, sem que caiba à outra parte qualquer direito de indenização.

ALTERAÇÃO DO CONTRATO

CLÁUSULA DÉCIMA QUINTA - A alteração incidente sobre o objeto do Contrato deve ser consensual e pode ser quantitativa, quando importa acréscimo ou diminuição do objeto do Contrato, ou qualitativa, quando a alteração diz respeito a características e especificações técnicas do objeto do Contrato.

PARÁGRAFO PRIMEIRO - A alteração quantitativa sujeita-se aos limites previstos nos § 1º e 2º do Artigo 81 da Lei nº 13.303/2016, devendo observar o seguinte:

a) A aplicação dos limites deve ser realizada separadamente para os acréscimos e para as supressões, sem que haja compensação entre os mesmos;

b) Deve ser mantida a diferença, em percentual, entre o valor global do Contrato e o valor orçado pelo **CONTRATANTE**.

Excepcionalmente a alteração qualitativa não se sujeitará aos limites previstos nos § 1º e 2º do Artigo 81 da Lei n. 13.303/2016, desde que observe os seguintes pressupostos:

a) Os encargos decorrentes da continuidade do Contrato devem ser inferiores aos da rescisão contratual e aos da realização de um novo procedimento licitatório;

b) As consequências da rescisão contratual, seguida de nova licitação e contratação, devem importar prejuízo relevante ao interesse coletivo a ser atendido pela obra ou pelo serviço;

c) As mudanças devem ser necessárias ao alcance do objetivo original do Contrato, à otimização do cronograma de execução e à antecipação dos benefícios sociais e econômicos decorrentes;

d) A capacidade técnica e econômico-financeira da **CONTRATADA** deve ser compatível com a qualidade e a dimensão do objeto contratual aditado;

e) A motivação da mudança contratual deve ter decorrido de fatores supervenientes não previstos e que não configurem burla ao processo licitatório;

f) A alteração não deve ocasionar a transfiguração do objeto originalmente contratado em outro de natureza ou propósito diverso.

PARÁGRAFO SEGUNDO - As alterações incidentes sobre o objeto devem ser:

a) Instruídas com memória de cálculo e justificativas de competência do fiscal técnico e do fiscal administrativo do **CONTRATANTE**, que devem avaliar os seus pressupostos e condições e, quando for o caso, calcular os limites;

b) As justificativas devem ser ratificadas pelo gestor do Serviço do **CONTRATANTE**;

c) Submetidas à área jurídica e, quando for o caso, à área financeira do **CONTRATANTE**;

PARÁGRAFO TERCEIRO - As alterações contratuais incidentes sobre o objeto e as decorrentes de revisão contratual devem ser formalizadas por termo aditivo firmado pela mesma autoridade que firmou o Contrato, devendo o extrato do termo aditivo ser publicado no sítio eletrônico do **CONTRATANTE**.



PARÁGRAFO QUARTO - Não caracterizam alteração do contrato e podem ser registrados por termo de apostilamento, dispensando a celebração de termo aditivo:

- a) A variação do valor contratual para fazer face ao reajuste de preços;
- b) As atualizações, as compensações ou as penalizações financeiras decorrentes das condições de pagamento previstas no Contrato;
- c) A correção de erro material havido no instrumento de Contrato;
- d) As alterações na razão ou na denominação social da **CONTRATADA**.

DAS SANÇÕES ADMINISTRATIVAS

CLÁUSULA DÉCIMA SEXTA - Pela inexecução total ou parcial do objeto, o **CONTRATANTE** poderá, garantido o contraditório e a ampla defesa, sem prejuízo das demais cominações previstas neste Contrato, aplicar as penalidades previstas nas leis nº 13.303/16:

- I – Advertência;
- II – Multa de 10% (dez por cento) sobre o valor global da contratação, pela inexecução total do ajuste;
- III – Multa diária de 0,2% (dois décimos por cento), calculado sobre o valor da respectiva fatura, quando houver atraso parcial na execução do objeto do contrato enquanto perdurar o inadimplemento;
- IV - Suspensão do direito de licitar e de contratar com o **CONTRATANTE** pelo prazo de até 02 (dois) anos;

PARÁGRAFO PRIMEIRO - O atraso na entrega dos serviços superior a 30 (trinta) dias consecutivos, poderá ensejar, a exclusivo critério do **CONTRATANTE**, a rescisão do Contrato.

PARÁGRAFO SEGUNDO - A rescisão do Contrato provocada pela **CONTRATADA** implicará, de pleno direito, a cobrança pelo **CONTRATANTE** de multa equivalente a 10% (dez por cento) do valor total contratado.

PARÁGRAFO TERCEIRO - Nenhuma penalidade será aplicada pelo **CONTRATANTE** sem o devido processo administrativo, assegurado o contraditório e a ampla defesa, no prazo de 10 (dez) dias úteis.

PARÁGRAFO QUARTO - A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança, facultada a defesa prévia, não isentará a obrigação de indenizar eventuais perdas e danos.

PARÁGRAFO QUINTO - O valor das multas apurado, após o processo administrativo, será descontado dos pagamentos eventualmente devidos ao **CONTRATANTE**.

PARÁGRAFO SEXTO - Inexistindo pagamento devido ao **CONTRATANTE**, ou sendo este insuficiente, caberá à parte contrária efetuar o pagamento do que for devido, no prazo máximo de 10 (dez) dias consecutivos, contados da data da comunicação de confirmação da multa, em depósito em conta corrente própria em nome do **CONTRATANTE**.

PARÁGRAFO SÉTIMO - Em não se realizando o pagamento nos termos definidos no Parágrafo acima, far-se-á a sua cobrança judicialmente.



DA RESCISÃO

CLÁUSULA DÉCIMA SÉTIMA - A rescisão do Contrato poderá ocorrer:

- I- Mediante distrato, pela inexecução parcial ou total do Contrato;
- II- Amigavelmente, por acordo entre as partes, desde que haja conveniência para a Administração, precedida de autorização escrita e fundamentada, mediante aviso prévio por escrito, de 30 (trinta) dias consecutivos;
- III- Judicialmente, nos termos da Legislação.

PARÁGRAFO PRIMEIRO - Sem prejuízo de outras Sanções, constituem motivos para rescisão por justa causa deste Contrato, pelo **CONTRATANTE** as situações descritas nos subitens abaixo:

- a. Paralisação injustificada dos serviços;
- b. O não cumprimento de Cláusulas contratuais, especificações ou prazos;
- c. A subcontratação, ainda que parcial, dos serviços objeto do Contrato;
- d. A cessão ou transferência do Contrato;
- e. O desatendimento às determinações da FISCALIZAÇÃO designada para acompanhar e fiscalizar a execução dos serviços;
- f. O cometimento reiterado de faltas na execução dos serviços;
- g. A decretação de falência, o pedido de recuperação judicial ou extrajudicial;
- h. A dissolução da sociedade.
- i. A alteração societária que modifique a finalidade ou o controle acionário ou, ainda, a estrutura da **CONTRATADA** que, a juízo do **CONTRATANTE**, inviabilize ou prejudique a execução deste Contrato;
- j. A prática de qualquer ato que vise fraudar ou burlar o fisco ou Órgão/entidade arrecadador/credor dos encargos sociais e trabalhistas ou de tributos;
- k. O descumprimento de quaisquer das condições ajustadas neste Contrato;
- l. A utilização pela **CONTRATADA** de mão-de-obra de menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e menores de 16 (dezesesseis) anos em qualquer trabalho, salvo na condição de aprendizes, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII do Art. 7º da Constituição Federal (Emenda Constitucional nº 20, de 1998);
- m. O conhecimento, ainda que, “a posteriori”, de fato ou ato que afete a idoneidade da **CONTRATADA** ou de seus sócios/cotistas ou de seus gestores ou ainda de seus representantes;
- n. Razões de interesse público;
- o. Ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditivo da execução deste Contrato;
- p. Deixar de comprovar sua regularidade fiscal, trabalhista, inclusive contribuições previdenciárias e depósitos de FGTS para com seus empregados;
- q. Utilizar em benefício próprio ou de terceiras informações sigilosas às quais tenha acesso por força de suas atribuições.

PARÁGRAFO SEGUNDO - O **CONTRATANTE** poderá, a qualquer tempo, mediante aviso com antecedência mínima de 30 (trinta) dias, denunciar o Contrato, para efeito de rescisão, sem que, por esse motivo, seja obrigado a suportar ônus de indenização, multa ou pagamento extra de qualquer natureza, salvo previsão em Lei.



PARÁGRAFO TERCEIRO - Também poderá ocorrer rescisão quando:

- a. Vier a ser declarada inidônea por qualquer órgão da Administração Pública;
- b. Vier a ser atingida por protesto de título, execução fiscal ou outros fatos que comprometam a sua capacidade econômico-financeira.

PARÁGRAFO QUARTO - A rescisão acarretará, de imediato, retenção dos créditos decorrentes deste Contrato, até o limite dos prejuízos causados ao **CONTRATANTE**.

PARÁGRAFO QUINTO - Na rescisão do Contrato, o **CONTRATANTE** aplicará à **CONTRATADA** multa prevista neste Contrato.

PARÁGRAFO SEXTO - Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados à **CONTRATADA** o contraditório e o direito à ampla defesa.

PARÁGRAFO SÉTIMO - As responsabilidades imputadas à **CONTRATADA**, por danos diretos decorrentes de ações delitivas perpetradas contra o **CONTRATANTE**, não cessam com a rescisão deste Contrato.

DAS GARANTIAS DOS MATERIAIS E SERVIÇOS

CLÁUSULA DÉCIMA OITAVA - A **CONTRATADA** obriga-se a dar garantia aos serviços e equipamentos conforme este termo de referência pelo prazo de 180 (cento e oitenta) dias, a contar da data da assinatura do Contrato, contra qualquer defeito de fabricação, incluindo avarias no transporte até o local de entrega, mesmo depois de ocorrida sua aceitação pelo **CONTRATANTE**. Durante esse período de garantia, a **CONTRATADA** prestará manutenção ao bem, de acordo com o seguinte esquema:

I. Durante o período da garantia, a **CONTRATADA** providenciará a reparação de eventual defeito ou substituição, no prazo máximo de 10 (dez) dias contado da data de notificação do defeito, sem ônus para o **CONTRATANTE**, seja com transporte do bem, peças, ferramentas, diárias de mão-de-obra, hospedagem e alimentação de técnicos, seguros, embalagem;

II. Findo tal prazo, sem a devida reparação dos serviços e equipamentos conforme este termo de referência, a **CONTRATADA** deverá substituir, em 24 (vinte e quatro) horas, por outro novo e original, entregando-a no mesmo local da anterior, tudo sem ônus, inclusive despesas com transporte, substituição e entrega;

III. A **CONTRATADA** deverá apresentar listagem das empresas credenciadas para prestação de assistência técnica corretiva durante todo o período da garantia, compreendendo no mínimo de 01 (uma) empresa credenciada em cada local para onde serviços e equipamentos conforme este Contrato serão destinados.

IV. Se o defeito encontrado não for resultante de mau uso ou negligência por parte de Prepostos do **CONTRATANTE**, este nada pagará pelo conserto/substituição do equipamento;

V. Se o bem entregue ao **CONTRATANTE** apresentar qualquer tipo de defeito ou não estiver em conformidade com as especificações deste Contrato, o mesmo deverá ser substituído no prazo máximo de 15 (quinze) dias consecutivos;

VI. Toda e qualquer despesas decorrentes da execução dos Serviços de Garantia aqui descritos, inclusive as substituições de produtos e/ou seus componentes, ficarão inteiramente a cargo da **CONTRATADA**, bem como a responsabilidade dos produtos e/ou seus componentes que estiverem sob sua guarda, ou sob a guarda de sua Assistência Técnica credenciada, arcando com quaisquer danos.

VII. A **CONTRATADA**, deverá apresentar um termo de garantia técnica por escrito com prazo de 30 (trinta) dias após a assinatura do Contrato.



DO SIGILO E RESTRIÇÕES

CLÁUSULA DÉCIMA NONA - É responsabilidade da **CONTRATADA** garantir absoluto sigilo sobre todos os processos, fórmulas, rotinas, objetos, informações, documentos e quaisquer outros dados que venham a ser disponibilizados pelo **CONTRATANTE** ao mesmo, em razão da execução do Contrato, oriundo desta contratação.

PARÁGRAFO PRIMEIRO - É responsabilidade da **CONTRATADA** garantir absoluto sigilo e confidencialidade sobre todos os processos, fórmulas, rotinas, objetos, informações, documentos, dados técnicos, comerciais e quaisquer outros elementos disponibilizados pelo **CONTRATANTE**, em razão da execução do contrato decorrente desta contratação.

PARÁGRAFO SEGUNDO - A **CONTRATADA** deverá observar integralmente os quesitos da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), responsabilizando-se pela proteção dos dados pessoais tratados no âmbito da execução contratual, de acordo com os princípios da finalidade, necessidade, adequação, segurança, prevenção e responsabilização.

PARÁGRAFO TERCEIRO – Em observância à LGPD e às normas complementares a **CONTRATADA** assinará, no ato da assinatura do Contrato, o documento denominado **Termo de Confidencialidade/Segurança da Informação - Anexo I** deste Contrato.

PARÁGRAFO QUARTO - A **CONTRATADA** compromete-se a adotar todas as medidas técnicas e administrativas necessárias para prevenir incidentes de segurança da informação e vazamento de dados, incluindo controles de acesso, criptografia, segregação de funções e registros de auditoria.

PARÁGRAFO QUINTO - É vedada à **CONTRATADA** a utilização das informações disponibilizadas pelo **CONTRATANTE** para qualquer outra finalidade que não seja a execução do objeto contratual, sob pena de aplicação das sanções previstas em contrato, sem prejuízo das responsabilidades civil, administrativa e penal cabíveis.

PARÁGRAFO SEXTO - A **CONTRATADA** deverá garantir a formalização de termo de Confidencialidade e Sigilo com todos os empregados envolvidos na prestação do serviço, conforme modelo disponibilizado no **Anexo IV - Termo de Responsabilidade e Confidencialidade do Empregado Terceirizado** deste Contrato.

DA VIGÊNCIA DO CONTRATO

CLÁUSULA VIGÉSIMA - O contrato terá vigência de **180 (cento e oitenta) dias** consecutivos e ininterruptos contados a partir de sua assinatura.

PARÁGRAFO ÚNICO - O Contrato poderá ser rescindido, a qualquer momento, desde que ocorra a conclusão da assinatura do Contrato proveniente da licitação em razão da proposta apresentada e comunicação feita pelo **CONTRATANTE** com 30 (trinta) dias de antecedência.

DO MODELO DE GESTÃO E FISCALIZAÇÃO DO CONTRATO

CLÁUSULA VIGÉSIMA PRIMEIRA - A Fiscalização da prestação dos serviços objeto da contratação será realizada pela Gerência de Infraestrutura e Produção - **GPROD-CORED**, que designarão representante do **CONTRATANTE** para o acompanhamento e Fiscalização do cumprimento das obrigações previstas neste Contrato.

PARÁGRAFO PRIMEIRO - O Contrato deverá ser executado fielmente pelas Partes, de acordo com as Cláusulas avençadas e as normas da Lei nº 13.303 de 2016, e cada parte responderá pelas consequências de sua inexecução total ou parcial.



PARÁGRAFO SEGUNDO - Em caso de impedimento, ordem de paralisação ou suspensão do Contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

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

PARÁGRAFO QUARTO - O **CONTRATANTE** poderá convocar representante da **CONTRATADA** para adoção de providências que devam ser cumpridas de imediato.

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

PARÁGRAFO SEXTO - Fiscalização: A execução do Contrato deverá ser acompanhada e fiscalizada pelo (s) fiscal (is) do Contrato, ou pelos respectivos substitutos.

PARÁGRAFO SÉTIMO - Fiscalização Técnica:

- a) O Fiscal Técnico do Contrato acompanhará a execução do Contrato, para que sejam cumpridas todas as condições estabelecidas no Contrato, de modo a assegurar os melhores resultados para a Administração;
- b) O Fiscal Técnico do Contrato anotará no histórico de gerenciamento do Contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.
- c) Identificada qualquer inexactidão ou irregularidade, o Fiscal Técnico do Contrato emitirá notificações para a correção da execução do Contrato, determinando prazo para a correção.
- d) O Fiscal Técnico do Contrato informará ao Gestor do serviço, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.
- e) No caso de ocorrências que possam inviabilizar a execução do Contrato nas datas aprazadas, o Fiscal Técnico do Contrato comunicará o fato imediatamente ao Gestor do Serviço.
- f) O Fiscal Técnico do Contrato comunicará ao Gestor do Serviço, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

PARÁGRAFO OITAVO - Fiscalização Administrativa:

- b) O Fiscal Administrativo do Contrato verificará a manutenção das condições de habilitação da **CONTRATADA**.
- c) Em caso de descumprimento de obrigações administrativas contratuais, como a ausência de garantias legais, desatualização de certidões, pendências trabalhistas ou descumprimento de Cláusulas contratuais não técnicas, o fiscal administrativo atuará tempestivamente na solução do problema, comunicando imediatamente ao gestor do contrato quando as medidas necessárias ultrapassarem sua competência direta;
- d) A Fiscalização administrativa, no âmbito desta contratação, deverá obedecer às seguintes rotinas específicas, considerando a natureza estratégica e contínua da prestação dos serviços de conectividade:

- i. Verificação periódica da validade da documentação de habilitação da **CONTRATADA** (balancetes, certidões negativas, apólices de seguro-garantia etc.);
- ii. Conferência da vigência e regularidade da garantia contratual, nos moldes exigidos pela Lei nº 13.303/2016;
- iii. Monitoramento da regularidade trabalhista e previdenciária dos profissionais alocados, quando aplicável, especialmente para técnicos residentes e equipes de campo que realizem suporte nas dependências do **CONTRATANTE**.
- iv. Acompanhamento do cumprimento das obrigações contratuais formais, tais como entrega de relatórios gerenciais, cronogramas de implantação, atas de reuniões técnicas, registros de ocorrências e documentações de visitas técnicas.
- v. Registro de ocorrências administrativas no histórico do contrato, com descrição precisa das ações adotadas e dos prazos para regularização.
- vi. Apoio ao gestor do serviço na elaboração de notificações formais e aplicação de penalidades administrativas, quando cabíveis, conforme previsto no instrumento contratual.
- vii. Comunicação prévia à área responsável sempre que forem identificados indícios de inexecução contratual, suspensão das atividades ou risco de descontinuidade dos serviços, especialmente nas localidades de maior criticidade operacional.

PARÁGRAFO NONO - Gestor do Serviço:

- a) O Gestor do serviço coordenará a atualização do processo de acompanhamento e Fiscalização do Contrato contendo todos os registros formais da execução no histórico de gerenciamento do Contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do Contrato para fins de atendimento da finalidade da administração.
- b) O Gestor do serviço acompanhará os registros realizados pelos Fiscais do Contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.
- c) O Gestor do serviço acompanhará a manutenção das condições de habilitação da **CONTRATADA**, para fins de pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.
- d) O Gestor do serviço emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e negócios quanto ao cumprimento de obrigações assumidas pela **CONTRATADA**, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.
- e) O Gestor do serviço tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela área competente para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).
- f) O Gestor do serviço deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.
- g) O Gestor do serviço deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela Fiscalização e gestão nos termos do Contrato.



PARÁGRAFO DÉCIMO - O acompanhamento e a Fiscalização da execução do Contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o cumprimento do ajuste, e serão exercidos por um ou mais representantes do **CONTRATANTE**.

PARÁGRAFO DÉCIMO PRIMEIRO - A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Contrato e na proposta.

PARÁGRAFO DÉCIMO SEGUNDO - A ausência ou omissão da Fiscalização do **CONTRATANTE** não eximirá a **CONTRATADA** das responsabilidades previstas neste Contrato.

DA VEDAÇÃO

CLÁUSULA VIGÉSIMA SEGUNDA - O presente Contrato não poderá ser, no todo ou em parte, objeto de cessão ou transferência.

PARÁGRAFO PRIMEIRO - Nos termos do Art. 7º do Decreto nº 7.203, de 04.06.2010, que dispõe sobre a vedação de nepotismo no âmbito da Administração Pública Federal, também é vedado à **CONTRATADA** utilizar, durante toda a vigência deste Contrato, mão de obra de cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o 3º (terceiro) grau, de empregado do **CONTRATANTE** que exerça cargo em comissão ou função de confiança, razão pela qual por meio do seu representante legal, a **CONTRATADA** assinará o **ANEXO II** deste Contrato.

DA MATRIZ DE RISCO

CLÁUSULA VIGÉSIMA TERCEIRA - A Matriz de Riscos consiste no documento que discrimina de forma clara e objetiva os riscos assumidos por cada uma das partes na celebração deste instrumento contratual e está disposto no **ANEXO VIII**, deste Contrato

DOS CRITÉRIOS DE SUSTENTABILIDADE

CLÁUSULA VIGÉSIMA QUARTA - A **CONTRATADA** se compromete a atender às diretrizes da Política de Responsabilidade Socioambiental do Banco da Amazônia – PRSAC, disponível em <https://www.bancoamazonia.com.br/component/edocman/prsac/viewdocument/5204> e a Política Geral de Contratações, disponível em <https://www.bancoamazonia.com.br/component/edocman/politica-geral-de-contratacoes/viewdocument/5727>, considerando os requisitos a seguir:

- Não permitir a prática de trabalho análogo ao escravo ou qualquer outra forma de trabalho ilegal, bem como implementar esforços junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam no mesmo sentido;
- Não empregar menores de 18 (dezoito) anos para trabalho noturno, perigoso ou insalubre, e menores de 16 (dezesesseis) anos para qualquer trabalho, com exceção a categoria de Menor Aprendiz, conforme **Anexo III** deste Contrato;
- Não permitir a prática ou a manutenção de discriminação limitativa ao acesso na relação de emprego, ou negativa com relação a sexo, origem, raça, cor, condição física, religião, estado civil, idade, situação familiar ou estado gravídico, bem como a implementar esforços nesse sentido junto aos seus respectivos fornecedores;

- Respeitar o direito de formar ou associar-se a sindicatos, bem como negociar coletivamente, assegurando que não haja represálias;
- Proteger e preservar o meio ambiente, bem como buscar prevenir e erradicar práticas que lhe sejam danosas, exercendo suas atividades em observância dos atos legais, normativos e administrativos relativos às áreas de meio ambiente, emanadas das esferas federal, estaduais e municipais e implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores;
- Desenvolver suas atividades em cumprimento à legislação ambiental, fiscal, trabalhista, previdenciária e social locais, bem como às Normas Regulamentadoras de saúde e segurança ocupacional e demais dispositivos legais relacionados a proteção dos direitos humanos, abstendo-se de impor aos seus colaboradores condições ultrajantes, sub-humanas ou degradantes de trabalho. Para o disposto desse artigo define-se: a) “Condições ultrajantes”: condições que expõe o indivíduo de forma ofensiva, insultante, imoral ou que fere ou afronta os princípios ou interesses normais, de bom senso, do indivíduo. b) “Condições sub-humanas”: tudo que está abaixo da condição humana como condição de degradação, condição de degradação abaixo dos limites do que pode ser considerado humano, situação abaixo da linha da pobreza. c) “Condições degradantes de trabalho”: condições que expõe o indivíduo à humilhação, degradação, privação de graus, títulos, dignidades, desonra, negação de direitos inerentes à cidadania ou que o condicione à situação de semelhante à escravidão;
- Atender à Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), observando quanto ao descarte adequado e ecologicamente correto;
- Apresentar conformidade com a legislação e regulamentos que disciplinam sobre a prevenção e combate à Lavagem de Dinheiro e ao Financiamento ao Terrorismo;
- Não ter sofrido sanções que implicam na restrição de participar de licitações ou de celebrar contratos com a Administração Pública, não constar registro da empresa e/ou sócios e representantes no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), atendendo às diretrizes anticorrupção;
- Adotar práticas e métodos voltados para a preservação da confidencialidade e integridade, atentando à Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018;
- O **CONTRATANTE** poderá recusar o recebimento de qualquer serviço, material ou equipamento, bem como rescindir imediatamente o contrato, sem qualquer custo, ônus ou penalidade, garantida a prévia defesa, caso se comprove que a contratada, subcontratados ou fornecedores utilizam-se de trabalho em desconformidade com as condições referidas nas Cláusulas supracitadas.

DA INTEGRIDADE, DA CONDUTA ÉTICA E DOS PROCEDIMENTOS ANTICORRUPÇÃO

CLÁUSULA VIGÉSIMA QUINTA - O Contrato oriundo da presente contratação deverá prever que as Partes declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas, a Lei de Improbidade Administrativa - Lei nº 8.429, de 02 de junho de 1992 e a Lei Anticorrupção - Lei nº 12.846, de 01 de agosto de 2013 e seus regulamentos e se comprometem a cumpri-las fielmente, por si e por seus sócios, administradores e colaboradores, bem como exigir o seu cumprimento pelos terceiros por elas contratados. Adicionalmente, as Partes declaram que tem e manterão até o final da vigência do contrato, oriundo desta contratação, um código de ética e conduta próprio, cujas regras se obriga a cumprir fielmente. Sem prejuízo da obrigação de cumprimento das disposições de seus respectivos códigos de ética e conduta, ambas as Partes desde já se obrigam, no exercício dos direitos e obrigações previstos no Contrato e no cumprimento de qualquer uma de suas disposições:



- I. Não dar, oferecer ou prometer qualquer bem de valor ou vantagem de qualquer natureza a agentes públicos ou a pessoas a eles relacionadas ou ainda quaisquer outras pessoas, empresas e/ou entidades privadas, com o objetivo de obter vantagem indevida, influenciar ato ou decisão ou direcionar negócios ilicitamente;
- II. Adotar as melhores práticas de monitoramento e verificação do cumprimento das leis anticorrupção, com o objetivo de prevenir atos de corrupção, fraude, práticas ilícitas ou lavagem de dinheiro por seus sócios, administradores, colaboradores e/ou terceiros por elas contratados;
- III. Respeitar e exigir que seus empregados respeitem, no que couber, os princípios éticos e os compromissos de conduta definidos no Código de Conduta Ética do **CONTRATANTE**, cujo teor poderá ser acessado no site www.bancoamazonia.com.br.

PARÁGRAFO PRIMEIRO - A comprovada violação de quaisquer das obrigações previstas nesta contratação é causa para a rescisão unilateral do Contrato, sem prejuízo da cobrança das perdas e danos causados à parte inocente.

PARÁGRAFO SEGUNDO - A aplicação das sanções previstas na Lei nº 12.84, de 2013 não afeta os processos de responsabilização e aplicação de penalidades decorrentes de atos ilícitos.

DO FORO

CLÁUSULA VIGÉSIMA SEXTA - Fica eleito o Foro da cidade de Belém, capital do estado do Pará, com renúncia a qualquer outro, por mais privilegiado que seja, para dirimir as questões que porventura surgirem na execução do presente Contrato.

E por estarem de pleno acordo as Partes reconhecem e concordam expressamente que a inserção de sua senha pessoal e/ou a utilização de outras formas de assinatura eletrônica. Inclusive biométricas, em plataformas digitais, como a "DocuSign", constitui forma legítima e suficiente para a confirmação de seus dados, comprovação de sua identidade e validade de sua declaração de vontade para assinar e celebrar o presente Contrato para que produza todos os seus efeitos de direito, conforme dispões e Legislação aplicável.

Belém/PA, Data da última assinatura eletrônica.

BANCO DA AMAZÔNIA S.A.

Assinado por:

Bruna Eline da Silva Cavalcante

BRUNA ELINE DA SILVA CAVALCANTE

Gerente Executiva da Gerência de Contratações
e Gestão Administrativa de Contratos - GECOG

CLARO S.A.

Assinado por:

Luciana Costa Conceição

LUCIANA COSTA CONCEIÇÃO

Gerente Executiva de Contas

ANEXO I

TERMO DE CONFIDENCIALIDADE E SIGILO DE DADOS E INFORMAÇÕES

Este Termo de Compromisso é celebrado entre:

BANCO DA AMAZÔNIA, Endereço Avenida Presidente Vargas, nº 800, Belém/Pará, inscrito no CNPJ/MF 04.902.979/0001-44, representado neste ato por sua Gerente Executiva da Gerência de Contratações e Gestão Administrativa de Contratos - GECOG, Sra. **BRUNA ELINE DA SILVA CAVALCANTE**, brasileira, solteira, bancária, portadora da Carteira de Identidade Profissional nº 25700 OAB/PA e CPF/MF 796.223.562-49, residente e domiciliada na Região Metropolitana de Belém/PA, abaixo assinado ("**CONTRATANTE**"), e a empresa **CLARO S.A.**, sociedade anônima de capital fechado, com registro na Junta Comercial do Estado de São Paulo (JUCESP) sob o NIRE 35.300.145.801, com sede em São Paulo/SP, na Rua Henri Dunant, nº 780, Torres A e B, Bairro Santo Amaro, CEP: 04.709-110, inscrita no CNPJ/MF sob o nº 40.432.544/0001-47, representada neste ato por Procuração pela sua Gerente Executiva de Contas, Sra. **LUCIANA COSTA CONCEIÇÃO**, brasileira, casada, gerente executiva de contas, portadora da Carteira de Identidade Profissional nº 14580D CRE/PA e do CPF/MF nº 802.396.502-63, abaixo assinado ("**CONTRATADA**"), **CONTRATANTE** e **CONTRATADA** em conjunto denominadas como Partes:

CONSIDERANDO QUE as Partes, por meio do Contrato nº 2025/227 estão estabelecendo uma relação jurídica para prestação de serviços de Comunicação por meio de **Rede Privada de Comunicação Multisserviço MPLS** com enlaces de transmissão, hardware, software para a interligação corporativa das redes locais (LAN) e Metropolitanas (MAN), abrangendo a Direção Geral, Superintendências, Agências, Postos Bancários e rede parceiros, com **Balanceamento Seguro de circuitos** e **Solução WIFI**, incluindo **Sistema de Gerenciamento e Monitoração WAN** e fornecimento de **Acessos a rede Internet** com proteção **Anti-DDoS Volumétrico**, **Anti-DDoS Camada de Aplicação**, **Segurança e proteção da rede LAN (NGFW)** e **Rede Dedicada de Alta Velocidade**, que necessariamente incluem o acesso, o conhecimento e o tratamento de dados e informações corporativas da **CONTRATANTE** pela **CONTRATADA**, além do uso de equipamentos, de recursos computacionais e outros que envolvam a possibilidade de divulgação de informações restritas, de exclusivo interesse da **CONTRATANTE**, sob a posse, guarda e domínio da **CONTRATADA**;

CONSIDERANDO QUE as Partes podem divulgar entre si informações classificadas como restritas e/ou sigilosas, conforme definido abaixo neste instrumento, sobre aspectos de seus respectivos negócios;

CONSIDERANDO QUE as Partes desejam ajustar as condições de revelação das Informações Restritas e/ou sigilosas, bem como definir as regras relativas ao seu uso e proteção;

RESOLVEM as Partes celebrar o presente Termo de Compromisso e Sigilo de Dados e Informações ("Termo"), o qual se regerá pelas considerações acima, bem como, **pelas considerações que forem pertinentes constantes na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) e nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).**

1. OBJETO

Este Termo tem por objeto exclusivo proteger as Informações Confidenciais que venham a ser fornecidas ou reveladas pelo **CONTRATANTE** à **CONTRATADA**, bem como disciplinar a forma pela qual elas devem ser utilizadas pela **CONTRATADA**.



1.1. Todas as informações ou dados revelados ou fornecidos, direta ou indiretamente, pela **CONTRATANTE** ou por terceiros em nome desta à **CONTRATADA**, ou obtida por esta de forma lícita, independentemente de divulgação explícita, em quaisquer meios de armazenamento ou transmissão e independente do formato, rotulação ou forma de envio, devem ser tratadas como Informações Confidenciais.

1.2. A **CONTRATADA** reconhece que as Informações Confidenciais são de propriedade exclusiva do **CONTRATANTE** ou são advindas de terceiros e estão sob sua responsabilidade.

1.3. As Informações Confidenciais poderão estar contidas e serem transmitidas por quaisquer meios, incluindo, entre outros, as formas escritas, gráfica, verbal, mecânica, eletrônica, digital, magnética ou criptográfica.

2. RESTRIÇÕES QUANTO À UTILIZAÇÃO DAS INFORMAÇÕES CONFIDENCIAIS

2.1. A **CONTRATADA** reconhece a importância de se manter as Informações Confidenciais em segurança e sob sigilo, mesmo após o término de vigência do presente Termo, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidas, reveladas, divulgadas ou utilizadas, sem prévia autorização do **CONTRATANTE**, a qualquer terceiro estranho a este Termo.

2.2. Sem prejuízo das demais obrigações previstas neste Termo, a **CONTRATADA** obriga-se a:

(i) Tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que lhe forem fornecidos pelo **CONTRATANTE** e preservar o seu sigilo, de acordo com a Legislação vigente;

(ii) Preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo ou comercializar a terceiros;

(iii) Não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito;

(iv) Não copiar ou reproduzir, por qualquer meio ou modo: (a) informações classificadas em qualquer grau de sigilo; (b) informações relativas aos materiais de acesso restrito do **CONTRATANTE** salvo autorização da autoridade competente.

(v) Não utilizar, reter, duplicar, modificar, adulterar, subtrair ou adicionar qualquer elemento das Informações Confidenciais que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo **CONTRATANTE** para finalidades específicas;

(vi) Não modificar ou adulterar as Informações Confidenciais fornecidas pelo **CONTRATANTE**, bem como não subtrair ou adicionar qualquer elemento a essas Informações Confidenciais;

(vii) Armazenar e transmitir as Informações Confidenciais digitais em ambiente seguro, com controle de acesso e mediante o uso de criptografia;

(viii) Devolver ao **CONTRATANTE**, ou a exclusivo critério dessa destruir, todas as Informações Confidenciais que estejam em seu poder em até 48h (quarenta e oito horas), contados da data da solicitação; e

(ix) Informar imediatamente o **CONTRATANTE** qualquer violação a este Termo.



3. PROTEÇÃO DE DADOS PESSOAIS

3.1. A CONTRATADA obriga-se a, sempre que aplicável, atuar em conformidade com a Legislação vigente sobre proteção de dados relativos a uma pessoa física identificada ou identificável ("Dados Pessoais") e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais"), bem como seguir as instruções informadas pelo **CONTRATANTE** quanto ao tratamento dos Dados Pessoais que teve acesso em função do presente Termo.

3.2. A CONTRATADA compromete-se a auxiliar o **CONTRATANTE**: i) com a suas obrigações judiciais ou administrativas, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança; e ii) no cumprimento das obrigações decorrentes dos Direitos dos Titulares dos Dados Pessoais, principalmente por meio de medidas técnicas e organizacionais adequadas;

3.3. Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da relação estabelecida com o **CONTRATANTE** ou na execução das atividades ligadas a este Termo, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade da relação negocial conforme as disposições acordadas, a **CONTRATADA** concorda em notificar formalmente este fato o **CONTRATANTE**, que terá o direito de resolver a relação negocial sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.

4. DISPOSIÇÕES GERAIS

4.1. A **CONTRATADA** declara estar ciente de que o manuseio inadequado das Informações Confidenciais, sua divulgação ou revelação não autorizada a quaisquer terceiros representarão, por si só, prejuízo ao patrimônio, à imagem e reputação do **CONTRATANTE**, e implicará em sua responsabilização civil ou criminal, de acordo com a violação verificada, obrigando-se ao ressarcimento das perdas e danos decorrente.

4.2. A inobservância de quaisquer das disposições de confidencialidade estabelecidas neste Termo sujeitará a **CONTRATADA**, além de sanções penais cabíveis, ao pagamento o **CONTRATANTE** e a terceiros pelas perdas e danos, diretos e indiretos, decorrentes do evento de descumprimento, facultada ainda o **CONTRATANTE** a rescisão do presente Termo e demais acordos que estiverem vigentes com a **CONTRATADA**.

4.3. Este Termo não impõe obrigações à **CONTRATADA** com relação às Informações Confidenciais que (i) já sejam lícita e comprovadamente de conhecimento da **CONTRATADA** anteriormente à da sua divulgação pelo **CONTRATANTE**; (ii) sejam ou venham a se tornar de conhecimento público, sem qualquer intervenção da **CONTRATADA** e (iii) sejam divulgadas à **CONTRATADA** por qualquer terceiro que as detenham em legítima posse, sem que isto constitua violação de dever de confidencialidade previamente assumido com o **CONTRATANTE**.

4.4. Se a **CONTRATADA** vier a ser obrigada a divulgar, no todo ou em parte, as Informações Confidenciais por qualquer ordem judicial ou autoridade governamental competente, a **CONTRATADA** poderá fazê-lo desde que notifique imediatamente o **CONTRATANTE**, para permitir que esta adote as medidas legais cabíveis para resguardo de seus direitos.

4.5. Se a **CONTRATADA**, na hipótese aqui tratada, tiver que revelar as Informações Confidenciais, divulgará tão somente a informação que foi legalmente exigível e envidará seus melhores esforços para obter tratamento de segredo para quaisquer Informações Confidenciais que revelar, nos precisos dispositivos deste Termo e da Lei.



4.6. A **CONTRATADA** concorda que não deve se opor à cooperação ou empenho de esforços com o **CONTRATANTE** para auxiliar na adoção das medidas judiciais competentes, sendo certo que nada poderá ser exigido ou solicitado a **CONTRATADA** que não esteja dentro dos estritos limites legais.

4.7. O presente Termo permanecerá em vigor por prazo indeterminado, independentemente da formalização de qualquer negócio entre as Partes.

4.8. Quaisquer alterações a este Termo somente terão validade e eficácia se forem devidamente formalizadas através de termo aditivo firmado entre as Partes.

4.9. O presente Termo será interpretado pela Legislação da República Federativa do Brasil e as Partes desde já elegem o Foro da Cidade de Belém, Estado do Pará, para dirimir qualquer controvérsia oriunda deste instrumento, salvo disposição específica pela legislação aplicável.

E por estarem de pleno acordo as Partes reconhecem e concordam expressamente que a inserção de sua senha pessoal e/ou a utilização de outras formas de assinatura eletrônica. Inclusive biométricas, em plataformas digitais, como a “DocuSign”, constitui forma legítima e suficiente para a confirmação de seus dados, comprovação de sua identidade e validade de sua declaração de vontade para assinar e celebrar o presente Contrato para que produza todos os seus efeitos de direito, conforme dispões e Legislação aplicável.

Belém/PA, Data da última assinatura eletrônica.

BANCO DA AMAZÔNIA S.A.

Assinado por:

Bruna Elíne da Silva Cavalcante

FB59D5B7727F4AA

BRUNA ELÍNE DA SILVA CAVALCANTE

Gerente Executiva da Gerência de Contratações
e Gestão Administrativa de Contratos - GECOG

CLARO S.A.

Assinado por:

Luciana Costa Conceição

1A49D0B4F0B74DF

LUCIANA COSTA CONCEIÇÃO

Gerente Executiva de Contas

ANEXO II**DECLARAÇÃO DE CONHECIMENTO DO TEOR DO DECRETO Nº. 7.203, DE 04.06.2010**

Para contratar com o **CONTRATANTE**, cujo objeto é a prestação de serviços técnicos de manutenção corretiva “on site” sob demanda e preventiva referente em 157 (cento e cinquenta e sete) Terminais de Autoatendimento (ATMs), modelo TMF 4100, instalados nas Unidades do Banco da Amazônia até o momento, mediante chamados registrados, a **CLARO S.A.**, sociedade anônima de capital fechado, com registro na Junta Comercial do Estado de São Paulo (JUCESP) sob o NIRE 35.300.145.801, com sede em São Paulo/SP, na Rua Henri Dunant, nº 780, Torres A e B, Bairro Santo Amaro, CEP: 04.709-110, inscrita no CNPJ/MF sob o nº 40.432.544/0001-47, representada neste ato por Procuração pela sua Gerente Executiva de Contas, Sra. **LUCIANA COSTA CONCEIÇÃO**, brasileira, casada, gerente executiva de contas, portadora da Carteira de Identidade Profissional nº 14580D CRE/PA e do CPF/MF nº 802.396.502-63, **DECLARA** que:

- a) Tem conhecimento do teor do Decreto nº. 7.203, de 04.06.2010, que dispõe sobre a vedação de nepotismo no âmbito da Administração Pública Federal; e
- b) Em cumprimento ao citado Decreto, não utilizará durante toda a vigência do contrato a ser firmado com o **CONTRATANTE** mão de obra de cônjuge, companheiro ou parente em linha reta ou colateral, por consanguinidade ou afinidade, até o 3º. (terceiro) grau, de agente público que exerça cargo em comissão ou função de confiança no Banco da Amazonia S. A.

Belém/PA, Data da última assinatura eletrônica.

CLARO S.A.

Assinado por:

1449D0B4F0BA4DE
LUCIANA COSTA CONCEIÇÃO
Gerente Executiva de Contas



ANEXO III

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE EMPREGADO MENOR NO QUADRO DA EMPRESA

Decreto 4.358, de 05.09.2002

CLARO S.A., sociedade anônima de capital fechado, com registro na Junta Comercial do Estado de São Paulo (JUCESP) sob o NIRE 35.300.145.801, com sede em São Paulo/SP, na Rua Henri Dunant, nº 780, Torres A e B, Bairro Santo Amaro, CEP: 04.709-110, inscrita no CNPJ/MF sob o nº 40.432.544/0001-47, representada neste ato por Procuração pela sua Gerente Executiva de Contas, Sra. **LUCIANA COSTA CONCEIÇÃO**, brasileira, casada, gerente executiva de contas, portadora da Carteira de Identidade Profissional nº 14580D CRE/PA e do CPF/MF nº 802.396.502-63, **DECLARA**, para fins do disposto na Lei 13.303 de 30 de Junho de 2016, acrescido pela Lei nº 9.854, de 27 de Outubro de 1999, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesesseis) dezesesseis anos.

***Ressalva: Emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz ().**

Belém/PA, Data da última assinatura eletrônica.

CLARO S.A.

Assinado por:

Luciana Costa Conceição

LUCIANA COSTA CONCEIÇÃO
Gerente Executiva de Contas

ANEXO IV

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE DO EMPREGADO TERCEIRIZADO

Eu, [NOME DO EMPREGADO], portador do CPF nº [NÚMERO DO CPF], declaro, como empregado da [RAZÃO SOCIAL DA CONTRATADA], estar ciente de minhas responsabilidades profissionais quanto à segurança dos recursos computacionais e das informações corporativas do Banco da Amazônia S.A., cujos acessos me serão franqueados para desempenho, exclusivo, das funções para as quais fui expressamente contratado e designado.

Por esse termo de responsabilidade e confidencialidade, comprometo-me a:

- a) Manter-me atualizado com a Política de Segurança da Informação e Cibernética e demais Políticas Internas e Normas de Segurança do CONTRATANTE;
- b) Manter o sigilo absoluto de minhas senhas de acesso à rede corporativa e a sistemas, estando ciente que minhas senhas são pessoais e intrasferíveis, cabendo a mim, exclusivamente, a guarda sigilosa, não sendo permitido compartilhar, revelar, salvar, replicar, publicar ou fazer uso não autorizado de minhas senhas;
- c) Manter sigilo absoluto de informações do CONTRATANTE que me sejam franqueados em função da minha atividade profissional;
- d) Manter vigilância dos materiais, máquinas, ferramentas e outros pertences de minha propriedade guardados no local dos serviços, quando forem prestados nas dependências do CONTRATANTE, além de zelar pelos equipamentos, materiais e quaisquer outros recursos de propriedade do CONTRATANTE colocados eventualmente à minha disposição, utilizando-os de maneira correta e cuidadosa e estritamente para os fins do cumprimento das minhas atividades;
- e) Manter sigilo das informações do CONTRATANTE ou de terceiros, classificadas como sigilosas, restritas e internas, não divulgando ou comercializando, interna ou externamente, a não ser quando devidamente autorizado;
- f) Não copiar, reproduzir, transferir ou usar indevidamente quaisquer informações do CONTRATANTE para qualquer outra finalidade que não seja a promoção dos serviços contratados, observando-se o disposto neste termo;
- g) Não utilizar, reter ou duplicar as informações que lhe forem fornecidas para criação de qualquer arquivo, lista ou banco de dados de sua utilização particular ou de quaisquer terceiros, exceto quando autorizada expressamente por escrito pelo CONTRATANTE;
- h) Não transferir as informações corporativas do Banco da Amazônia para outros meios de armazenamento (físicos e nuvem), não autorizados pelo Banco, para fins particulares, sob pena de responsabilização por vazamento de dados;
- i) Não utilizar as informações de forma que possa configurar concorrência desleal com o CONTRATANTE, tampouco explorá-las em outros negócios ou oportunidades comerciais, sem prévia e expressa autorização do CONTRATANTE;
- j) Não comentar, compartilhar ou publicar na Internet ou em mídias sociais, ou qualquer plataforma de armazenagem aberta de dados, como repositórios digitais, quaisquer informações relacionadas à prestação de serviços que tem junto ao CONTRATANTE a não ser que tenha havido prévia e expressa autorização;
- k) Não realizar qualquer atividade relacionada a captura de áudio, vídeo ou imagens dentro das dependências do CONTRATANTE, exceto quando relacionada a atividade contratada;



- l) Cessar o uso, bem como devolver, imediatamente após o término do Contrato, todos os materiais, informações, documentos, recursos (inclusive crachás, usuários de acesso a sistemas etc.) do CONTRATANTE que tenham me sido emprestados ou de qualquer forma disponibilizados;
- m) Acessar os ambientes do CONTRATANTE, sejam eles físicos ou lógicos, estritamente para a execução da prestação dos serviços contratados;
- n) Respeitar às leis vigentes de direito autoral e Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) bem como as demais leis, normas e políticas de proteção de dados pessoais corporativas;
- o) Manter sigilo de dados pessoais cujo CONTRATANTE figura como controlador ou operador, não divulgando ou comercializando, interna ou externamente, a não ser quando devidamente autorizado;
- p) Seguir as instruções recebidas do CONTRATANTE em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes e aplicáveis, devendo garantir sua licitude e idoneidade;
- q) Tratar todos os Dados Pessoais como restritos, exceto se já eram de conhecimento público sem qualquer contribuição sua, ainda que a relação contratual entre as Partes venha a ser resolvida, e independentemente dos motivos que derem causa;
- r) Notificar o CONTRATANTE assim que tomar conhecimento de qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (i) de qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; (ii) de quaisquer exposições ou ameaças em relação à conformidade com a proteção de Dados Pessoais; (iii) ou em período menor, se necessário, de qualquer ordem de Tribunal, autoridade pública ou regulador competente;
- s) Ter a ciência de que o CONTRATANTE monitora seus ambientes físicos e lógicos visando a eficácia dos controles implantados, a proteção de seu patrimônio e reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes ligados à segurança da informação;
- t) Comunicar imediatamente ao meu Gerente imediato ou diretamente ao fiscal do contrato qualquer falha, suspeita ou ameaça por mim detectada aos ativos do CONTRATANTE, como informações, recursos de tecnologia da informação, ambientes físicos, imagem e reputação;
- u) Respeitar às leis vigentes de direito autoral e no que couber, ter como ação os princípios e práticas descritos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no que tange à segurança, a privacidade e o tratamento das informações, bem como, adotar ações no presente para a plena observância da referida lei no momento de sua vigência;

Sendo estas responsabilidades estendidas:

- a) Para fora das dependências do CONTRATANTE e fora dos horários normais de trabalho quando na execução de trabalho remoto, em cliente ou em outra dependência do CONTRATANTE;
- b) Por tempo indeterminado, mesmo após o término da relação profissional da CONTRATADA com o CONTRATANTE, no que tange a não divulgação e comercialização de informações sigilosas e informações pessoais;

Estou ciente que transgressões destas normas são consideráveis faltas graves e que poderei responder civil e penalmente por quaisquer prejuízos causados ao Banco da Amazônia.

[Local], XX de XXXX de XXXX.

[NOME DO EMPREGADO TERCEIRIZADO]

ANEXO V

REQUISITOS MÍNIMOS DE SEGURANÇA PARA SISTEMAS ADQUIRIDOS

REQUISITOS GERAIS DE SEGURANÇA PARA A CONTRATADA

A **CONTRATADA** deverá assinar, no início do contrato, o Termo de Confidencialidade e Sigilo que terá como objetivo definir as regras relativas ao tratamento, acesso, proteção e revelação das informações corporativas do Banco da Amazônia (BASA).

Todos os empregados da empresa contratada que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato deverão assinar o Termo de Responsabilidade e Confidencialidade do Empregado Terceirizado. O referido termo deverá ser entregue ao gestor do contrato antes do início das atividades do profissional.

A **CONTRATADA** deverá:

- I. Adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade do BASA;
- II. Comunicar com antecedência mínima de 15 (quinze) dias ao BASA qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do BASA, porventura colocados à disposição para realização dos serviços contratados;
- III. Manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo BASA a tais documentos;
- IV. Não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do BASA, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos;
- V. Manter seus empregados devidamente informados das normas disciplinares do BASA, bem como das normas de utilização e de segurança das instalações e do manuseio dos documentos;
- VI. Manter empregados devidamente identificados por meio de crachá funcional quando no ambiente do BASA;
- VII. Garantir que seus empregados conheçam a POL 304 - Política de Segurança da Informação e Comunicações e de Segurança Cibernética do BASA;
- VIII. Assumir inteira responsabilidade, pelos danos causados diretamente à administração ou a terceiros, incluindo prejuízos financeiros, decorrentes de sua culpa ou dolo, quando da não observância de requisitos mínimos de segurança no desenvolvimento de seus produtos e serviços;
- IX. Assumir inteira responsabilidade por quaisquer danos ou prejuízos causados ao BASA e a terceiros, incluindo prejuízos financeiros, por dolo ou culpa, de seus empregados, decorrentes dos serviços ora contratados;
- X. Garantir e manter total e absoluto sigilo sobre as informações manuseadas as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis;



XI. Não repassar a terceiros, em nenhuma hipótese, qualquer informação sobre a arquitetura e/ou documentação, assim como dados e/ou metadados trafegados, produtos desenvolvidos e entregues, ficando responsável juntamente com o BASA por manter a segurança da informação relativa aos dados e procedimentos durante a execução das atividades e em período posterior ao término da execução do Contrato;

XII. Assumir inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do BASA através do manuseio de sistemas e manipulação de dados, praticado por seus empregados, desde que devidamente comprovado;

XIII. Providenciar para que os produtos e artefatos da contratação sejam entregues em perfeito estado, com a segurança necessária, garantindo o transporte, o seguro, a entrega e a implantação nos locais indicados pelo BASA sem quaisquer danos, avarias ou ônus adicionais para o BASA.

COMPLIANCE PARA SERVIÇOS EXECUTADOS EM NUVEM

A contratada deve garantir que a legislação brasileira prevaleça sobre qualquer outra, de modo que o BASA tenha todas as garantias legais enquanto tomador do serviço e proprietário das informações, se hospedadas na nuvem.

A **CONTRATADA** deverá:

XIV. cumprir integralmente as diretrizes da Resolução CMN 4.893/21;

XV. fornecer acesso ao BASA aos dados e às informações a serem processados ou armazenados pela **CONTRATADA**;

XVI. Assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador;

XVII. Apresentar conformidade com a norma ABNT NBR ISO/IEC 27001:2013 referente aos serviços de computação em nuvem e aos data centers que hospedem esses serviços ou, alternativamente, demonstrar atender os objetivos e controles da referida norma, mediante apresentação de políticas, procedimentos, e outros documentos. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao BASA promover diligência destinada a esclarecer ou complementar informações;

XVIII. Fornecer ao BASA acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador, relativos aos procedimentos e aos controles utilizados na execução dos serviços a serem contratados;

XIX. Fornecer informações e recursos de gestão para possibilitar o monitoramento dos serviços a serem prestados;

XX. Assegurar, enquanto o contrato estiver vigente, a identificação e a segregação dos dados dos clientes do BASA por meio de controles físicos ou lógicos e forneça ao BASA documentos e/ou relatórios que evidenciem o cumprimento desta exigência;

XXI. Assegurar a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do BASA;

XXII. Adotar um padrão de identidade federada para permitir o uso de tecnologia **single sign-on** no processo de autenticação dos usuários do serviço de nuvem, o qual deve ser acompanhado de autenticação multifator (MFA).

XXIII. Registrar e armazenar, pelo período de um ano, todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações.



XXIV. Apoiar o BASA, quando necessário, nas atividades de investigação de incidentes de cibersegurança. Isso inclui fornecer prontamente informações e recursos necessários para a investigação, como logs, registros de eventos e relatórios de auditoria.

XXV. Adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, caso o serviço a ser contratado seja relativo ao serviço de execução de aplicação por meio da internet;

XXVI. Garantir que o ambiente seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados por outros usuários do serviço em nuvem;

XXVII. Assegurar que toda atualização do sistema seja previamente analisada e homologada antes que possa ser instalada/configurada, além de dispor de documentação de todas as alterações realizadas no serviço e/ou sistema mediante processos formalizados de Gestão e Mudanças;

XXVIII. Assegurar a adoção de medidas de segurança para a transmissão e armazenamento dos dados e das informações processados ou armazenados pelo prestador, e fornecer ao BASA evidências da adoção das referidas medidas;

XXIX. Notificar ao BASA sobre a subcontratação de serviços relevantes para a prestação do serviço contratado;

XXX. Notificar ao BASA sobre a intenção de interromper a prestação de serviços com pelo menos trinta dias de antecedência da data prevista para a interrupção;

XXXI. Conceder o acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

XXXII. Manter o BASA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;

XXXIII. Dispor de Plano de Comunicação de Incidentes e/ou dashboards com informações referentes a saúde dos serviços oferecidos de incidentes que possam ocorrer, informando o BASA os casos de incidentes de segurança da informação, assim considerados os eventos não previstos ou não desejados que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do BASA;

XXXIV. realizar a análise e gestão de riscos de segurança de informação. A análise deve ter periodicidade no mínimo mensal e deve ser apresentado um plano de gestão de riscos contendo: metodologia utilizada, riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes;

XXXV. Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção;

XXXVI. desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços ou envolvendo dados pessoais de empregados e/ou clientes do BASA;

XXXVII. Realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) e auditorias por terceira parte reconhecidamente confiável, disponibilizando relatório comprobatório a cada três meses para o BASA;



XXXVIII. Prover mecanismo de acesso protegido aos dados, por meio de comunicação criptografada, garantindo que apenas aplicações e usuários autorizados tenham acesso;

XXXIX. Deverá fornecer, sempre que solicitado pelo BASA, cópias dos logs de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de Application Programming Interface (API), caso haja, para análise de segurança e auditorias;

XL. Dispor de recursos e soluções técnicas que garantam a segurança da informação dos dados do BASA, incluindo os seguintes itens: solução de controle de tráfego de borda do tipo firewall (norte-sul, leste/oeste, e de aplicações), solução de prevenção e detecção de intrusão (IDS/IPS), antivírus, anti-malware, solução anti-DDoS, solução de gestão de logs, solução de gestão integrada de pacotes de correção (patches), solução de correlação de eventos de segurança (SIEM);

XLI. Realizar backups e salvaguardas dos conteúdos das comunicações realizadas por meio da solução e permitir a consulta desses dados;

XLII. Garantir a exclusividade de direitos, por parte do BASA, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como **backups** de segurança.

XLIII. Comprometer-se a preservar os dados do BASA contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (backups) destes dados fora do território brasileiro, devendo informar imediatamente e formalmente à BASA qualquer tentativa, inclusive por meios judiciais, de acesso por parte de outra nação a estes dados;

XLIV. Operar o serviço dentro do uso proposto, com desempenho razoável e exigindo o mínimo possível de permissões dos demais sistemas do BASA, além de proteger os dados transmitidos por meio dele, quando necessário;

XLV. Atestar informações referentes a medidas adotadas em proteção de dados pessoais, devendo ser capaz de demonstrar:

XLVI. As diretrizes de tratamento;

XLVII. O modo de atendimento a solicitações de titulares de dados pessoais;

XLVIII. As medidas protetivas para garantia da confidencialidade dos dados pessoais;

XLIX. As medidas protetivas durante as comunicações com o BASA;

L. O registro de atividades de tratamento de dados pessoais;

LI. A solicitação de autorização na subcontratação de terceiros para atividades de tratamento de dados pessoais;

LII. As medidas de devolução / descarte dos dados.

LIII. A partir do ponto de entrada/saída da internet nos datacenters do provedor de nuvem ofertados, a contratada deverá observar:

LIV. Inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei;

LV. Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

LVI. Não fornecimento a terceiros de dados do BASA, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;



LVII. Fornecer ao BASA, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do BASA.

LVIII. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo BASA, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se que:

LIX. Pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

LX. A informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, desde que em conformidade com a Resolução CMN 4.893/21.

LXI. A empresa deve garantir a adequação e a adoção de medidas pelo BASA, em decorrência de qualquer determinação do Órgãos Governamentais aos quais o BASA é subordinado que impacte sobre o Contrato vigente.

LXII. A **CONTRATADA** deve manter o BASA permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

LXIII. É vedado o uso de informações do BASA pela contratada para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

LXIV. Em caso de extinção do Contrato, a contratada deverá transferir os dados e as informações processados ou armazenados por ele ao novo prestador de serviços ou ao BASA e, após a confirmação da integridade e da disponibilidade dos dados e informações recebidos, os excluir.

LXV. Em caso da decretação de regime de resolução do BASA pelo Banco Central do Brasil, a **CONTRATADA** deverá:

LXVI. conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações que estejam em poder da empresa contratada; e

LXVII. Notificar previamente o responsável pelo regime de resolução sobre sua intenção de interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção. A **CONTRATADA** obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução. A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência do BASA.

REQUISITOS DE ARQUITETURA, DESIGN E MODELAGEM DE AMEAÇAS

O sistema, com recursos web, deverá incorporar, no mínimo, proteção contra:

LXVIII. **Controle de acesso falho:** as restrições sobre o que os usuários autenticados têm permissão para fazer muitas vezes não são aplicadas de forma adequada. Os invasores podem explorar essas falhas para acessar funcionalidades e/ou dados não autorizados, como acessar contas de outros usuários, visualizar arquivos confidenciais, modificar dados de outros usuários, alterar direitos de acesso etc.

LXIX. **Falhas criptográficas:** Muitos aplicativos da web e APIs não protegem adequadamente os dados sigilosos, como dados pessoais e financeiros. Os invasores podem roubar ou modificar esses dados fracamente protegidos para conduzir fraude de cartão de crédito, roubo de identidade ou outros crimes. Os dados sigilosos podem ser comprometidos sem proteção extra, como criptografia em repouso ou em trânsito, e requerem precauções especiais quando trocados com o navegador.

LXX. Injeção: Injeções ocorrem quando dados informados pelo usuário são enviados para um interpretador como parte de um comando ou uma query. O dado malicioso do atacante faz o interpretador executar comandos que não deveria ou modificar dados. Algumas das injeções mais comuns são SQL, NoSQL, OS command, Mapeamento Relacional de Objeto (ORM), LDAP e Expression Language (EL) ou Object Graph Navigation Library (OGNL). O conceito é idêntico entre todos. A revisão do código-fonte é o melhor método para detectar se os aplicativos são vulneráveis a injeções.

LXXI. Design inseguro: O design seguro é uma cultura e metodologia que avalia constantemente as ameaças e garante que o código seja desenvolvido e testado de forma robusta para evitar métodos de ataque conhecidos. O design seguro requer um ciclo de vida de desenvolvimento seguro, alguma forma de padrão de design seguro ou biblioteca ou ferramenta de componentes de estradas pavimentadas e modelagem de ameaças.

LXXII. Configuração incorreta de segurança: geralmente é o resultado de configurações padrão inseguras, configurações incompletas ou ad hoc, armazenamento em nuvem aberta, cabeçalhos HTTP configurados incorretamente e mensagens de erro detalhadas contendo informações confidenciais. Não apenas todos os sistemas operacionais, estruturas, bibliotecas e aplicativos devem ser configurados com segurança, mas também devem ser corrigidos / atualizados em tempo hábil.

LXXIII. Componentes vulneráveis e desatualizados: componentes, como bibliotecas, estruturas e outros módulos de software, são executados com os mesmos privilégios do aplicativo. Se um componente vulnerável for explorado, esse tipo de ataque pode facilitar a perda séria de dados ou o controle do servidor. Aplicativos e APIs que usam componentes com vulnerabilidades conhecidas podem minar as defesas do aplicativo e permitir vários ataques e impactos.

LXXIV. Falhas de identificação e autenticação: as funções do aplicativo relacionadas à autenticação e gerenciamento de sessão são frequentemente implementadas incorretamente, permitindo que os invasores comprometam senhas, chaves ou tokens de sessão ou explorem outras falhas de implementação para assumir as identidades de outros usuários temporária ou permanentemente.

LXXV. Falhas de software e integridade de dados: As falhas de software e integridade de dados estão relacionadas ao código e à infraestrutura que não protegem contra violações de integridade. Por exemplo, quando objetos ou dados são codificados ou serializados em uma estrutura que um invasor pode ver e modificar, logo é vulnerável à desserialização insegura. Outro exemplo é quando um aplicativo depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs).

LXXVI. Registro (logging) e monitoramento insuficientes: registro (logging) e monitoramento insuficientes, juntamente com a integração ausente ou ineficaz com a resposta a incidentes, permite que os invasores ataquem ainda mais os sistemas, mantenham a persistência, ganhem acesso em mais sistemas e adulterem, extraiam ou destruam dados.

LXXVII. Server-Side Request Forgery (SSRF): As falhas de SSRF ocorrem sempre que um aplicativo web busca um recurso remoto sem validar a URL fornecida pelo usuário. Ele permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de ACL de rede.

LXXVIII. Validação de entrada inadequada: o produto recebe entradas ou dados, mas não valida ou valida incorretamente se a entrada possui as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos devam satisfazer apenas o esperado pela aplicação.

LXXIX. Caracteres Especiais ou maliciosos: caracteres especiais são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros. Garanta que apenas entradas válidas, esperadas e apropriadas sejam processadas pelo Sistema.



LXXX. A solução deverá possuir conformidade com o OWASP TOP 10 vigente visando assegurar a segurança dos dados, gerar confiança entre os usuários, prevenir perdas financeiras e cumprir regulamentações de segurança, proporcionando a integridade e a credibilidade necessárias para um site ou aplicativo.

A solução não deve ser baseada nos frameworks Wordpress ou Joomla.

Deverá ser imposto o menor privilégio em conexões com o banco de dados ou outros sistemas de back-end.

A **CONTRATADA** deverá realizar configuração segura (hardening) do servidor web no qual a aplicação está hospedada e deverá assegurar que servidores web da aplicação estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmark mais atual.

As seguintes flags e procedimentos relacionados deverão ser adotados em relação às configurações do cabeçalho para a comunicação entre o servidor e o cliente:

LXXXI. A aplicação deverá instruir o browser a só permitir acesso via HTTPS. Deverá ser ativado o HTTP Strict Transport Security (HSTS) adicionando um cabeçalho de resposta com o nome 'Strict-Transport-Security' e o valor 'max-age = expireTime', em que expireTime é o tempo em segundos que os navegadores devem lembrar que o site só deve ser acessado usando HTTPS. O max-age deve ser de pelo menos 31536000 segundos (1 ano);

LXXXII. O cabeçalho X-Content-Type-Options deverá estar configurado como 'nosniff' para todas as páginas da web;

LXXXIII. A aplicação deverá retornar o cabeçalho X-Frame-Options com o valor DENY ou SAMEORIGIN, que permitirá "framing" das páginas conforme SAME ORIGIN;

LXXXIV. A aplicação deverá ter o CSP habilitado enviando os cabeçalhos de resposta Content-Security-Policy, conforme políticas que atenda critérios de segurança na implementação dessa diretiva;

LXXXV. A aplicação deverá ter o cabeçalho X-XSS-Protection desabilitado, por meio da configuração do seu valor como 0 (zero);

LXXXVI. A aplicação não deverá possuir os cabeçalhos "fingerprinting": X-Powered-By, Server, X-AspNet-Version;

LXXXVII. A aplicação deverá forçar content-type para as respostas. Se a aplicação retorna json, a resposta content-type da aplicação deverá ser application/json;

LXXXVIII. Os tipos de conteúdo text/*, / + xml e application/xml também devem especificar um conjunto de caracteres seguro (por exemplo, UTF-8, ISO-8859-1);

LXXXIX. O conteúdo da aplicação não poderá ser incorporado a um site de terceiro por padrão;

XC. O Cross-Origin Resource Sharing (CORS) e cabeçalho Access-Control-Allow-Origin deverão utilizar uma lista de permissão restrita de domínios e subdomínios confiáveis para correspondência e não oferecer suporte à origem "null", e validar os dados inseridos pelo usuário;

XCI. O cookie emitido pela aplicação deverá possuir os atributos SameSite, SECURE e HttpOnly;

XCII. A aplicação deverá utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações.



Antes da entrada em produção, a solução passará por homologação quanto a sua segurança. Quaisquer eventuais vulnerabilidades identificadas pela equipe do BASA serão tratadas como defeito de software e deverão obrigatoriamente ser corrigidas pela CONTRATADA.

Realizar configuração segura do servidor web, também conhecido como hardening. Assegurar que servidores WEB estejam configurados seguindo as melhores práticas de segurança, com base no CIS Benchmarks.

Utilizar apenas o HTTPS com certificados válidos e cifras adequadas é fundamental para garantir a segurança online. O HTTPS protege a confidencialidade dos dados, os certificados válidos asseguram a autenticidade do site e a configuração correta de cifras previne vulnerabilidades, sendo essencial para proteger dados e a integridade das comunicações.

REQUISITOS DE ARMAZENAMENTO DE DADOS E PRIVACIDADE

Os recursos de armazenamento de credenciais do sistema deverão ser utilizados para armazenar dados restritos e sigilosos, como dados pessoais, credenciais de usuário ou chaves criptográficas

Dados restritos e sigilosos não deverão:

- ser exibidos em mensagens de erro;

- XCIII. ser armazenados fora do contêiner da aplicação ou de recursos de armazenamento de credenciais do sistema;

- XCIV. ser armazenados em texto claro, como um banco de dados não criptografado;

- XCV. aparecer nos logs de aplicação;

- XCVI. ser compartilhados com terceiros, exceto se for uma parte necessária da arquitetura;

- XCVII. ser expostos através de mecanismos IPC (Inter-process Communication);

- XCVIII. ser armazenados localmente ou em arquivos temporários no dispositivo. Em vez disso, os dados deverão ser recuperados de um terminal remoto quando necessário e mantidos apenas em memória.

A aplicação não deverá exibir mensagens de erro detalhadas que possa expor informações privilegiadas.

Senhas ou PINs de acesso não deverão ser expostos através da interface de usuário.

Credenciais de acesso não deverão ser armazenadas dentro do código-fonte do sistema.

Será obrigatória a validação, a filtragem e o tratamento de todos os dados inseridos pelo usuário.

Toda requisição de acesso ao banco de dados deverá passar por processo de validação de autorização.

Será vedada a filtragem de dados no cliente.

Não deverá ser utilizado o método GET (URLs) para o envio de dados restritos ou sigilosos ou para a realização transações financeiras.

O método HTTP deverá ser utilizado de acordo com a operação: GET (read), POST (create), PUT/PATCH (replace/update), e DELETE (delete).

Será proibida a utilização de dados sensíveis (credenciais de acesso, senhas, tokens ou API keys) na URL, deverá ser utilizado cabeçalho Authorization.

Toda requisição de acesso à API deverá passar por processo de validação de autorização.

Um mecanismo de validação de entrada padrão deverá ser utilizado para validar todos os dados em tamanho, tipo, sintaxe e regras de negócio antes de exibi-los ou armazená-los.

Deverá ser utilizada a estratégia de validação do tipo Whitelist.

Será obrigatória a validação content-type de dados publicados (POST) aceitáveis (por exemplo application/x-www-form-urlencoded, multipart/form-data, application/json etc.).



Entradas inválidas deverão ser rejeitadas, ao invés de se tentar sanitizar dados impróprios/maliciosos.

REQUISITOS DE AUTENTICAÇÃO

O sistema deve possuir controle de acesso dos usuários baseado em papéis, usuários e funções.

O sistema deve possuir mecanismo de múltiplo fator de autenticação (MFA);

O sistema deve ser capaz de admitir integração com MS-AD (Microsoft Active Directory) do BASA para login único de usuário (Single Sign On = SSO).

As senhas deverão ser gravadas em banco de dados de forma criptografada.

A tela de log-on não deverá exibir a senha que está sendo informada.

O sistema não deverá armazenar ou transmitir senhas em texto plano.

A tela de entrada dos sistemas deverá validar as informações fornecidas pelo usuário somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não deverá indicar qual parte do dado de entrada está correta ou incorreta.

Em caso de tentativa de log-on inválida, o sistema deverá exibir uma mensagem genérica e nunca exibir as mensagens "usuário inexistente" ou "senha incorreta", de modo a não fornecer mensagens que permitam a um usuário não autorizado deduzir informações de acesso.

Todo acesso administrativo deverá ser restrito e deverá ser garantido o acesso apenas aos usuários autorizados.

Deverá ser utilizado HTTPS para envio de credenciais.

Os sistemas não deverão passar ID de sessão por método HTTP GET.

Deverá ser utilizado sempre o método HTTP POST para a requisição de autenticação.

Será obrigatória a utilização do parâmetro "state" com hash aleatório no processo de autenticação do OAuth.

Será proibido o uso de Basic Authentication.

As autorizações de acesso deverão ser validadas, garantindo que nenhum usuário acessará o que não foi previamente definido em seu perfil.

O processo de login deve ser iniciado através de uma página com um novo cookie de sessão.

Todos os endpoints do sistema deverão ser protegidos por autenticação.

Será proibido o incremento de IDs automaticamente. No lugar, deverá ser utilizado UUID.

REQUISITOS DE GERENCIAMENTO DE SESSÃO DO USUÁRIO

As sessões deverão ser invalidadas pelo terminal remoto após um período de, no máximo, 15 minutos de inatividade e os tokens de acessos devem expirar.

O controle de sessão deverá ser tratado pelo servidor e apenas a persistência dele no cliente.

Os sistemas deverão implementar token de sessão por requisição com alta aleatoriedade, devendo ser utilizados tokens personalizados e aleatórios em todos os formulários e URLs que não serão automaticamente enviadas pelo navegador.

Toda as páginas deverão ter um link para o logout o qual, ao clicar, o sistema deverá realizar o logout sem antes questionar o usuário. O logout deve destruir todo o estado da sessão no lado servidor e os cookies no lado cliente.

Será proibido o uso de "response_type=token".

Dados de usuários, atributos e políticas utilizados pelos controles de acesso, não podem ser manipulados pelos usuários finais, a menos que especificamente autorizado na arquitetura do projeto.

O sistema deverá utilizar o princípio do menor privilégio, os usuários só devem ser capazes de acessar funções, arquivos de dados, URLs, controladores, serviços e outros recursos, para os quais possuam autorização específica.



Em caso de sistemas que utilizam JWT (JSON Web Token):

XCIX. Será obrigatório o uso de chaves randômicas (JWT Secret);

C. Será proibido armazenar dados confidenciais em tokens JWT.

CI. Será proibida a extração do algoritmo do cabeçalho (deverá ser validado no back-end);

CII. Deverá ser utilizado no back-end o algoritmo RS256;

CIII. Será obrigatório regras de time-out de sessão do usuário de 15 minutos, access token de 3 minutos e refresh token de 8 horas.

REQUISITOS DE COMUNICAÇÃO DE REDE

O sistema deverá ser capaz de suportar a pilha dupla IPV4 e IPV6.

Todas as comunicações externas entre os servidores do sistema e os clientes deverão ser encriptadas.

O sistema deverá utilizar criptografia para as comunicações externas entre os servidores do sistema e os clientes. Os dados deverão ser criptografados na rede utilizando somente TLS 1.2 ou superior.

O sistema não deverá permitir o uso do SSL, TLS 1.0 e TLS 1.1.

Deve-se usar os seguintes algoritmos: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256), SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 e SHAKE256.

Será vedada a utilização de cifras com vulnerabilidades divulgadas e/ou conhecidas.

As requisições deverão ser limitadas (através de rate limit ou outra solução semelhante), a fim de se evitar ataques de DoS (negação de serviço) ou força bruta.

Deverá ser utilizada a validação de "redirect_url" no servidor para permitir apenas URL's da *whitelist*.

Tráfegos HTTP deverão ser redirecionados para HTTPS.

A propriedade "readOnly" deverá ser configurada como "true" em esquemas de objeto para todas as propriedades que podem ser recuperadas por meio de APIs, mas nunca deverão ser modificadas.

Os modos de depuração do servidor da Web ou de aplicativos e da estrutura de aplicativos deverão ser desativados em produção para eliminar recursos de depuração, consoles de desenvolvedor e divulgações de segurança não intencionais.

REQUISITOS DE RESPOSTAS HTTP

Os cabeçalhos HTTP ou qualquer parte da resposta HTTP não deverão expor informações detalhadas da versão dos componentes do sistema.

A aplicação deverá retornar os seguintes códigos:

CIV. 405 Method Not Allowed: sempre que um método solicitado não for apropriado para o recurso solicitado

CV. 406 Not Acceptable: sempre que o formato suportado não for correspondido. Requisições content-type deverão ser validadas para permitir apenas o formato suportado (por exemplo application/xml, application/json etc.)

CVI. HTTP 200: código de resposta do status de sucesso do HTTP, indica que a solicitação foi bem-sucedida;

CVII. HTTP 302: indica que o recurso solicitado foi movido temporariamente para a URL fornecida pelo cabeçalho Location.

CVIII. HTTP 401: para qualquer ação não autorizada no sistema.

CIX. HTTP 429: para solicitações que excedam o limite de requisição permitido.



CX. HTTP 415: para solicitações contendo cabeçalhos de tipo de conteúdo ausentes ou inesperados

A aplicação deverá ter defesas contra ataques de poluição de parâmetro HTTP, especialmente se a estrutura do aplicativo não faz distinção sobre a origem dos parâmetros de solicitação (GET, POST, cookies, cabeçalhos ou variáveis de ambiente).

Redirecionamentos e encaminhamentos de URL deverão permitir apenas destinos que aparecem em uma lista de permissões ou deverão mostrar um aviso ao redirecionar para conteúdo potencialmente não confiável.

A aplicação deverá ter proteção contra ataques do tipo SSRF, validando ou higienizando dados não confiáveis ou metadados de arquivos HTTP, como nomes de arquivos, campos de entrada de URL, listas de protocolos, domínios, caminhos e portas.

REQUISITOS DE AUDITORIA

A solução deve dispor de logs de eventos para fins de auditoria, incluindo todas as ações administrativas e ações envolvendo os itens arquivados e pesquisados no que tange o arquivamento, visualização, recuperação e remoção de itens.

A solução deve dispor de logs com registro de informações a serem utilizadas na depuração e verificação de falhas da solução, mantendo o registro de toda atividade de arquivamento e recuperação realizada, inclusive para os processos de auditoria realizados.

A solução deve permitir a configuração de usuários (auditores), com permissão de monitorar (auditar) e acessar grupos específicos de caixas postais e/ou todas as mensagens arquivadas.

A solução deve suportar a geração e armazenamento de logs no formato IPV4 e IPV6.

As aplicações deverão implementar um sistema de *logging* que permita auditorias e investigações de incidentes de segurança, fraudes e casos de abuso.

A identificação do usuário, ou ID, deverá ser única, isto é, cada usuário deverá ter uma identificação própria.

Os sistemas de informação e suas respectivas infraestruturas deverão ser configurados de modo a registrar um critério mínimo de informações de logging e auditoria, contendo, no mínimo:

CXI. Operações de login e logout;

CXII. Tentativas de login malsucedidas;

CXIII. Acesso a telas cujo conteúdo é sigiloso, em segredo de justiça, possua dados pessoais ou bancários;

CXIV. Operações de inclusão, alteração ou exclusão de registros no banco de dados;

CXV. Execução de jobs e tarefas automatizadas;

CXVI. Criação, leitura, atualização ou exclusão de informações sigilosas;

CXVII. Mudanças de configurações no sistema, na rede ou em serviços (inicialização, suspensão e reinicialização de serviços), inclusive a instalação de patches e atualizações de softwares;

CXVIII. Acesso aos bancos de dados de fonte interna e externa;

CXIX. Falhas que resultem no fechamento anormal da aplicação, especialmente devido à exaustão de recurso ou atingimento do limite de um recurso (como memória do CPU, conexões de rede, espaço no disco etc.);

CXX. Acesso e alteração de trilhas de auditoria;

CXXI. Registros de tráfego de dados de fontes internas e externas; e

CXXII. Registros de processos internos relacionados às atividades do negócio.

Os registros dos eventos deverão incluir, no mínimo, as seguintes informações:

CXXIII. Identificação inequívoca do autor/ativo que realizou a atividade;



CXXIV. Sistema onde ocorreu ou foi observada a atividade (logger/observador do evento);

CXXV. tela (página) do sistema de onde a operação foi realizada;

CXXVI. Tipo de atividade ocorrida (tipo de evento/ação);

CXXVII. Data, hora e fuso horário, observando os mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB)", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);

CXXVIII. Retorno do sistema em caso de falhas ou sucesso na ação;

CXXIX. Identificador da instância (para sistemas clusterizados);

CXXX. Para operações de inserção, alteração ou exclusão, o tipo da operação, nome da tabela que foi manipulada, ID do registro e, se for o caso, valores anterior e atual de cada campo;

CXXXI. Parâmetros informados pelo usuário (ex: parâmetros repassados aos métodos GET ou POST);

CXXXII. Tempo de resposta do sistema;

CXXXIII. Para execução de jobs e tarefas automatizadas, armazenar o resultado da operação; falha, sucesso, cancelada etc.; e

CXXXIV. Endereço IP, nome do dispositivo, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

A aplicação não deve registrar credenciais ou detalhes de pagamento.

Os tokens de sessão só devem ser armazenados em logs de forma irreversível e com hash.

Será vedado o envio de informações sensíveis (ex: credenciais de acesso) para logs.

A solução não deverá registrar logs de auditoria em banco de dados da aplicação.

As aplicações deverão registrar logs de rastreamento distribuído (distributed tracing) de requisição.

As aplicações deverão gerar logs em formato que permita a completa identificação dos fluxos de dados

As aplicações deverão registrar eventos relevantes de segurança, incluindo eventos de autenticação bem-sucedidos e com falha, falhas de controle de acesso, falhas de desserialização e falhas de validação de entrada.

A solução deve garantir que todas as fontes de tempo estão sincronizadas com a hora e fuso horário corretos.

Dados de registro devem ser sanitizados para evitar ataques de injeção de registro.

REQUISITOS PARA APIs

A codificação de API deverá incorporar, no mínimo, proteção contra:



- a) Broken Object Level Authorization**
- b) Broken User Authentication**
- c) Excessive Data Exposure**
- d) Lack of Resources & Rate Limiting**
- e) Broken Function Level Authorization**
- f) Mass Assignment**
- g) Security Misconfiguration**
- h) Injection (Injection flaws, tais como SQL e NoSQL, Command Injection etc.)**
- i) Improper Assets Management**
- j) Insufficient Logging & Monitoring**
- k) Conformidade com o OWASP Top 10 API Security Risks em vigor**

Deverão ser utilizadas as classes Encoder e Validator da OWASP ESAPI (Enterprise Security API)

Deve ser imposto o menor privilégio quando se conectar ao banco de dados ou outros sistemas de back-end.

O banco de dados não deverá ser acessado por outro canal que não seja a aplicação

Os URLs da API não deverão expor informações confidenciais, tais como a chave da API, tokens de sessão etc.

Objetos serializados deverão usar verificações de integridade ou criptografados para evitar a criação de objetos hostis ou adulteração de dados.

Todos os endpoints acessíveis ao público devem usar um Certificado Digital que tenha sido assinado por uma Autoridade de Certificação aprovada e dentro do prazo de utilização.

Devem ser aplicadas políticas de limitação de taxa (ratelimit) para evitar o abuso da API.

Toda entrada pelo usuário por parâmetros da aplicação ou de forma manipulada em qualquer outra parte da aplicação, deverá ser validada, garantindo as propriedades necessárias para processar os dados de forma segura e correta. Garanta que os dados inseridos deveram satisfazer apenas o esperado."

A solução deve garantir que apenas entradas válidas, esperadas e apropriadas sejam processadas, pois caracteres especiais ou maliciosos são usados para explorar falhas como: SQL injection, XSS, Template Injection, entre outros.

ANEXO VI ESPECIFICAÇÕES TÉCNICAS

LOTE 01

1. REDE IP MULTIMEDIA

- 1.1. A Rede IP Multimídia deverá fazer QoS, fim a fim (CPE a CPE, incluindo a priorização dentro do backbone da CONTRATADA), priorizando as aplicações conforme suas criticidades, que serão definidas pelo CONTRATANTE após assinatura do contrato, em toda a rede MPLS do CONTRATANTE.
- 1.2. A Rede IP Multimídia consiste das unidades listadas no **ANEXO B**, interligadas através de uma rede com arquitetura VPN IP/MPLS e topologia lógica em full-mesh.
- 1.3. A Rede de Acesso consiste na interligação das unidades prediais de forma dedicada e exclusiva com a porta do backbone MPLS da CONTRATADA através de uma “nuvem” de camada de 2 (dois) aos Pontos de Concentração do CONTRATANTE.
- 1.4. Caso solicitado pelo CONTRATANTE, a CONTRATADA deverá restringir a comunicação lógica de determinadas unidades prediais a um conjunto de unidades previamente definidas (restrição de acesso lógico a partir de faixas de endereçamento IP, portas TCP e UDP).
- 1.5. A CONTRATADA deverá restringir a comunicação lógica de determinadas unidades prediais em até 07 (sete) dias consecutivos, a partir da formalização de solicitação pela CONTRATANTE.
- 1.6. O limite de atuação da CONTRATADA será a interface LAN do roteador que será conectado ao switches/hubs do CONTRATANTE.
- 1.7. Com relação à solução de alimentação e proteção elétrica, a CONTRATADA será responsável pelo fornecimento e interligação dos no-breaks gerenciados para suportar os equipamentos de sua propriedade, com o provimento de todos os recursos e instalações necessários, como bastidor e quadro de energia próprio exclusivo para este fim.
- 1.8. As especificações constantes deste Termo de Referência consideram que as soluções de telecomunicações a serem contratadas deverão ter alta qualidade, disponibilidade, desempenho, segurança e contingência no site central da CONTRATANTE ou onde ela indicar.
- 1.9. A CONTRATADA deverá providenciar a configuração lógica necessária para que a comunicação entre unidades prediais ocorram através da sua Rede de Acesso e backbone, em ambos os sentidos.
- 1.10. A CONTRATADA deverá se comprometer com o atendimento das futuras unidades prediais, a critério do CONTRATANTE, nas mesmas condições técnicas e de preço oferecidas ao CONTRATANTE para o objeto deste Termo de Referência desde que haja viabilidade técnica.
- 1.11. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer unidade predial, de acordo com a lei 10.303/16.
- 1.12. A Rede IP Multimídia deverá transportar dados, vídeo e voz sobre o protocolo IP conforme modelo de QoS a ser definido entre o CONTRATANTE e a CONTRATADA após assinatura do contrato.

- 1.13.** A CONTRATADA deverá utilizar em sua solução roteadores, que possibilitem a geração de estatísticas de uso dos enlaces por endereços IP origem/destino, por protocolo de camada 4 e por porta TCP/UDP origem/destino.
- 1.14.** A rede deverá suportar roteamento de tráfego IP multicast, em conformidade com os seguintes padrões:
 - a) RFC 2362, PIM-SM (Protocol Independent Multicast-Sparse Mode);
 - b) RFC 2236, Internet Group Management Protocol, Version 2;
 - c) RFC 2933, Internet Group Management Protocol MIB.
- 1.15.** A CONTRATADA deverá prestar os serviços de comunicação de dados, por meio de VPN IP/MPLS conforme os seguintes padrões:
 - a) RFC 2547, BGP/MPLS VPNs
 - b) RFC 2447, Diff Serv Code Point
 - d) RFC 2917, A Core MPLS IP VPN Architecture;
 - e) draft-ietf-l3vpn-rfc2547bis, BGP/MPLS IP VPNs.
- 1.16.** A topologia lógica da rede VPN IP/MPLS criada será do tipo full-mesh. O CONTRATANTE poderá, a seu critério, definir unidades prediais com conectividade lógica diferente de full-mesh (por exemplo, ponto-a-ponto ou partial-mesh).
- 1.17.** Quando solicitada pelo CONTRATANTE a CONTRATADA deverá implementar a conectividade lógica diferente de full-mesh em toda a rede com prazo de operacionalização das alterações a ser acordado entre as partes sendo que a reunião inicial para definição dos prazos e ajustes na rede deverá ser feita em no máximo dois dias consecutivos a partir da formalização de solicitação pelo CONTRATANTE.
- 1.18.** Os circuitos físicos de rede da CONTRATADA deverão ser configurados com QoS e deverão utilizar os protocolos listados abaixo:
 - 1.18.1. Velocidades de 512Kbps até 2Mbps: MLPPP (Mult Link PPP)
 - 1.18.2. Velocidades acima de 2Mbps:
 - MLPPP (no caso de um bundle de seriais: n x 2Mbps)
 - PPP (no caso da interface POS)
 - ETHERNET (Fast ou Giga-Ethernet)
- 1.19.** A CONTRATADA deve disponibilizar em todos os sites o protocolo de roteamento dinâmico BGP.
- 1.20.** A rede de comunicação de dados deverá ter garantia de desempenho, segurança, e suporte a diversos protocolos e permitir a utilização de endereçamento IP privativo.
- 1.21.** A rede da CONTRATADA deverá ter suporte ao uso de certificado digital privativo pelo CONTRATANTE.
- 1.22.** Requisitos de qualidade de Serviço (QoS)
 - 1.22.1. A solução da CONTRATADA deverá suportar a arquitetura DiffServ, incluindo DiffServ sobre redes MPLS conforme os seguintes padrões:
 - a) RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 Headers;
 - b) RFC 2475, An Architecture for Differentiated Services;



- c) RFC 2597, Assured Forwarding PHB Group;
- d) RFC 2598, An Expedited Forwarding PHB;
- e) RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services.

1.22.2. De acordo com as prioridades e níveis de serviços requisitados, os diferentes tipos de tráfego que cursarão por meio da Rede IP Multimídia deverão ser classificados nas classes de serviços (DiffServ), conforme descrito a seguir:

TIPO DE APLICAÇÃO	DESCRIÇÃO
a) Tempo Real Voz e Vídeo	Aplicações de voz e vídeo sensíveis a retardo (delay) e variações de retardo (jitter), que exigem priorização de tráfego e reserva de banda;
b) Missão Crítica	Aplicações interativas críticas para o negócio, que exigem entrega garantida, reserva de banda e tratamento prioritário;
c) Dados Alta Prioridade	Aplicações que necessitam de latência controlada – aplicações transacionais (ex: Base de Dados, SAP, PeopleSoft, Siebel, Financial, B2B, Supply Chain Management, Ariba, Microsoft SQL, DLSw+) e aplicações interativas (ex: Messenger, Net Meeting, Telnet, Citrix, PlaceWare);
d) Dados Média Prioridade	Aplicações que apresentam característica de rajada – Ex: Streaming de vídeo, E-mail (Lotus Notes, Outlook, SMTP, IMAP, etc), transferência de arquivos grandes (FTP), sincronização de base-de-dados, backups
e) Dados Baixa Prioridade	Aplicações não críticas com mensagens de tamanho muito variado e não imprescindíveis para o atendimento imediato.
f) Gerenciamento	Aplicações de gerenciamento de redes e de sistemas que necessitam de uma banda mínima para atividades de suporte técnico;
g) Classe Default	Reservado

Tabela 1

1.22.3. As políticas de QoS serão posteriormente definidas pelo CONTRATANTE em conjunto com a CONTRATADA para aplicação em cada site da rede, com prazo de operacionalização das alterações a ser acordado entre as partes sendo que a reunião inicial para definição dos prazos e ajustes na rede deverá ser feita em no máximo dois dias úteis a contar das assinaturas do Contrato de Prestação do Serviço.

1.22.4. Em todos os circuitos de acesso devem ser habilitado o QoS, sendo obrigatório, no mínimo a definição de aplicações de baixa prioridade e de gerenciamento, as demais classes podem ser configuradas ou não de acordo com a necessidade e escolha da CONTRATADA.

1.22.5. O CONTRATANTE poderá solicitar a qualquer momento a modificação nas configurações de QoS (classificadores, marcadores, escalonadores, policiamento, shaping, dentre outros) dos roteadores CPE, quando aplicável.

- 1.22.6. A CONTRATADA deverá modificar as configurações de QoS dos roteadores CPE e dos terminais remotos com prazo de operacionalização das alterações a ser acordado entre as partes sendo que a reunião inicial para definição dos prazos e ajustes na rede deverá ser feita em no máximo dois dias consecutivos a partir da formalização de solicitação pela CONTRATANTE.
- 1.22.7. A CONTRATADA deve garantir que o tráfego Real-Time seja inferior ou igual a 50% da banda total da interface para não comprometer outras aplicações da rede do CONTRATANTE.
- 1.22.8. A CONTRATADA deve garantir uma reserva máxima de banda de 97% para o tráfego das aplicações do CONTRATANTE em sua rede de acesso visando garantir a reserva de 3% para a classe default (supervisão da rede).

1.23. PADRÕES DE ENDEREÇAMENTO IP, ROTEAMENTO E INTERCONEXÃO DA REDE IP MULTIMÍDIA E REDE DE ACESSO

- 1.23.1. A CONTRATANTE será responsável pelo mapa de endereçamento IP adotado na Rede IP Multimídia e na Rede de Acesso.
- 1.23.2. A CONTRATANTE poderá utilizar no interior de sua rede o plano de endereçamento IP que preferir. Entretanto, a CONTRATADA deverá projetar e implementar a solução de forma a permitir a utilização do plano de endereços fornecido pela CONTRATANTE nas redes locais das unidades prediais.
- 1.23.3. A especificação da arquitetura de roteamento será definida pela CONTRATANTE, com a aprovação da CONTRATADA.
- 1.23.4. A CONTRATADA deverá projetar e implementar uma solução de roteamento que atenda aos requisitos de conectividade, contingência, balanceamento automático de tráfego e interconexão, baseada em roteamento dinâmico.
- 1.23.5. A solução de roteamento deverá ser projetada e implementada de forma escalável permitindo o crescimento da rede.
- 1.23.6. A solução de roteamento deverá permitir a convergência da rede em um tempo menor que 15 segundos para o caso de mudança topológica da rede causada por falha(s) em enlace(s) ou equipamento(s) de backbone.

1.24. REQUISITOS DE CONTINGÊNCIA

- 1.24.1. O site central Primário e o site Secundário (backup) deverão ser obrigatoriamente atendidos por fibra óptica em anel com redundância automática, sendo que os acessos do anel devem ser realizados por caminhos distintos até o ponto de presença (POP) da CONTRATADA.
- 1.24.2. Todos os elementos do core da rede deverão ser duplicados tanto no site Principal como no site Secundário, como por exemplos roteadores, backhaul, switches, gatekeepers, firewall, IPS.
- 1.24.3. As unidades principais e Secundárias deverão utilizar roteadores CPE distintos e duplicados com balanceamento automático de carga entre eles.
- 1.24.4. Os acessos da unidade Principal e Secundária deverão estar interligados diretamente aos roteadores de borda distintos da CONTRATADA, obedecendo aos requisitos abaixo:



- a) Alta disponibilidade através de uma solução de contingência atendida por roteadores duplicados e interconectados um ao outro através de conexão Fast Ethernet, conectados a cada um dos enlaces, operando com protocolo de redundância e operando com balanceamento automático de tráfego (exemplo: GLBP – *Gateway Load Balancing Protocol*, BGP – *Border Gateway Protocol*);
 - b) Na ocorrência de falha ou intermitência no funcionamento de um roteador CPE, a contingência deverá ser acionada automaticamente e proteger o tráfego que era cursado pelo(s) elemento(s) em falha em até 5 segundos.
 - c) Após a solução da falha causadora do contingenciamento, o tráfego deverá retornar automática e imediatamente para a situação anterior à falha;
- 1.24.5. Para o atendimento da unidade Principal e Secundária, os dois enlaces deverão ter capacidades idênticas na velocidade mínima de 2 x 155 Mbps/s para site Principal e 2 x 100 Mbps/s para site Secundário, por enlace, e operar com balanceamento automático de tráfego, portanto se houver falha em um enlace ou CPE todo o tráfego será transportado através do enlace remanescente sem perda de qualidade.

1.25. SISTEMA DE GERENCIAMENTO E MONITORAÇÃO

- 1.25.1. A **CONTRATADA** deverá disponibilizar uma solução de Gerência de Rede e Serviços abrangendo todo o serviço prestado e contemplando as áreas funcionais de gerência de Falhas, Desempenho, Configuração e de Nível de Serviço que deverá fornecer, no mínimo, as seguintes funcionalidades nas redes IP Multimedia, Internet, Dedicada:
- a) Geração e emissão de relatórios gerenciais que permitam o acompanhamento da qualidade dos serviços, dos níveis de serviços contratados (SLA) e dos chamados técnicos.
 - b) A Gerência de Rede e Serviços da CONTRATADA deverá abranger todos os seus roteadores CPE, inclusive no-breaks gerenciados, necessários para a prestação dos serviços de rede.
 - c) A Gerência de Rede e Serviços será de responsabilidade da CONTRATADA que deverá atuar de forma pró-ativa, antecipando-se aos problemas na rede e garantindo a qualidade do serviço estabelecida no Acordo de Nível de Serviço (SLA), realizando abertura automática de chamados, com respectivo acompanhamento e fechamento, relacionados com indisponibilidade e desempenho nos serviços de rede e gerenciamento de rede, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano.
 - d) Qualquer ocorrência de queda ou perda de qualidade dos serviços contratados deverão ter a condução dos chamados técnicos atualizados a cada 30 minutos no máximo;
- 1.25.2. A CONTRATADA é responsável por fornecer, dimensionar e configurar os equipamentos, sistemas e ferramentas necessárias para provimento da solução de Gerenciamento de Rede e Serviços.
- 1.25.3. Quaisquer recursos como links e equipamentos necessários a implementação da solução de gerência será de total responsabilidade da CONTRATADA;

- 1.25.4. As manutenções preventivas e corretivas e a atualização da infraestrutura de gerenciamento, bem como o suporte técnico deverão ser de responsabilidade e despesas da CONTRATADA.
- 1.25.5. A CONTRATANTE reservar-se-á o direito de designar preposto(s) para atuar em seu nome para o acompanhamento da gerência da rede, podendo este(s) preposto(s) cumprir(em) as obrigações da CONTRATANTE para este fim, sob supervisão da CONTRATANTE, incluindo, mas não limitado a recebimento de dados relativos ao gerenciamento da rede, realização de auditoria, apuração dos indicadores, validação de faturas e gerenciamento dos contratos de prestação de serviços.
- 1.25.6. Os dados e informações armazenados, conjuntamente com o modelo de dados poderão ser solicitados pela CONTRATANTE, a qualquer tempo, à CONTRATADA que deverá disponibilizá-los no prazo máximo de 5 (cinco) dias consecutivos, em meio definido pela CONTRATANTE e/ou na base de dados da solução de gerência (carga dos dados extraídos e removidos).
- 1.25.7. A solução de monitoração e gerenciamento deve possuir as seguintes características básicas.
- a) Monitoração pró-ativa dos links e roteadores.
- O serviço de monitoração pró-ativa deve ser feito em regime 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia. Uma vez detectada e diagnosticada a falha ou previsão de falha, deve ser disparada ação corretiva para solução do problema. São exemplos de falhas detectadas pela monitoração pró-ativa dos dispositivos: taxa de erros acima do limite, intermitência, queda de linha, linha inativa, e equipamentos com interface “down”.
- b) Abertura da reclamação
- Uma vez detectada e diagnosticada a falha ou previsão de falha, deverá ser aberto de forma automática a reclamação (Trouble-ticket) no centro de gerência da **CONTRATADA**.
- O primeiro contato com o centro de gerência da **CONTRATANTE** deverá ser feito em até 15 (quinze) minutos pela **CONTRATADA**, após ser verificado um evento ou alarme de falha e feita uma seccionalização do evento visando identificar a origem do problema e seus respectivos sintomas, objetivando agilizar sua solução. Feito isto, deverá ser realizado contato com a **CONTRATANTE** de modo a comunicar a ocorrência do evento, como também obter uma confirmação da **CONTRATANTE** de que o problema não está sendo causado por uma falha de responsabilidade da mesma, como falta de energia ou equipamento desligado.
- c) Consulta aos dados de configuração (links, designações, etc.) e inventário.
- A **CONTRATADA** deverá apresentar informações relativas a informações dos sites, localidades, equipamentos gerenciados (hardware e software), conexões físicas: portas, velocidade, endereçamento IP, informações sobre serviços: designação dos serviços contratados e gerenciados, CPE's, razão social etc.
- 1.25.8. O gerenciamento da rede será feito pelo centro de gerência da **CONTRATADA** que deverá estar disponível, 24 horas por dia, 07 dias por semana, 365 dias ao ano.



2. ACESSO FÍSICO

- 2.1. A CONTRATADA deverá garantir um tempo médio de desempenho mensal de latência para enlaces terrestre menor ou igual que 150ms e para enlaces satélite (SCPC) menor ou igual a 650 ms (nenhum enlace poderá ter duplo salto).
- 2.2. As tecnologias de acesso a serem utilizadas nos meios de comunicação devem atender as seguintes características:
 - a) Os circuitos atendidos por meio terrestres e satélites devem ser síncronos, dedicados e transparentes a protocolo.
 - b) Os circuitos atendidos por meio satélite utilizados como acesso a rede IP Multimedia, não devem utilizar qualquer tipo de multiplexação, devendo, necessariamente, ser atendido através de circuitos tipo SCPC ("Single Channel Per Carrier").
 - c) O meio físico de acesso dos circuitos concentradores (Primário e Secundário), por questões de qualidade e escalabilidade e disponibilidade, deve ser fornecido por meio de fibra óptica em anel com contingência automática, garantindo assim a continuidade da prestação do serviço em caso de interrupção em um dos segmentos do acesso. Para os sites remotos os acessos poderão ser atendidos por fibra óptica ou par metálico ou rádio acesso ou acesso satélite.
- 2.3. Os serviços a serem fornecidos devem estar dentro dos padrões em conformidade com as diretrizes do CONTRATANTE.
- 2.4. A CONTRATADA deverá prover uma rede logicamente independente e isolada de qualquer rede de terceiros, inclusive da Internet. O isolamento deverá ser realizado no nível 2 (dois) do modelo OSI. Esta garantia deverá ser implementada fim-a-fim.
- 2.5. A relação de endereços dos pontos de acesso à rede, com as respectivas especificações de larguras de banda e outras características é apresentada Pelo Banco..
- 2.6. A CONTRATADA deverá disponibilizar a infraestrutura necessária de acesso para atender às necessidades de comunicação de dados do CONTRATANTE.
- 2.7. A CONTRATADA fornecerá uma rede de comunicação de dados com garantia de velocidade e fornecimento de acesso de acordo com os quantitativos previstos Peço Banco.
- 2.8. O acesso ao PoP da CONTRATADA poderá ser realizado através de um desses protocolos: HDLC, PPP, ATM ou ETHERNET, desde que por meios não estatísticos, onde não haja compartilhamento de banda desde o equipamento roteador até a porta de entrada do backbone da CONTRATADA. Os links e as portas de acesso ao centro de roteamento da CONTRATADA deverão ser exclusivos e dedicados, não podendo haver compartilhamento com outros usuários;
- 2.9. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados.
- 2.10. O CONTRATANTE terá o direito de verificar a correta aplicação dessas políticas, através da realização de auditorias periódicas remotas e in-loco, dos ambientes físicos e lógicos da CONTRATADA.
- 2.11. Essa ação tem como intuito a prevenção de incidentes de segurança para garantir os níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do CONTRATANTE.

3. EQUIPAMENTOS CPE

- 3.1. Os roteadores deverão ser dimensionados, fornecidos, instalados, configurados, mantidos, gerenciados e operado pela CONTRATADA e deverá ser garantido o desempenho e os níveis de serviços contratados.
- 3.2. Todas as atualizações e correções (patches) de softwares necessários para o cumprimento dos requisitos exigidos neste Termo de Referência deverão ser realizadas sem ônus adicionais para o CONTRATANTE.
- 3.3. Os roteadores deverão ser da mesma marca, pertencendo ao mesmo fabricante para atendimento de toda a rede IP Multimedia, inclusive no *Core* da rede.
- 3.4. Os roteadores deverão ser fornecidos com todos os componentes, cabos, módulos e acessórios necessários ao seu perfeito funcionamento.
- 3.5. A CONTRATADA deverá habilitar em todos os roteadores o protocolo SNMP, com uma comunidade de leitura para acesso do CONTRATANTE ou seu preposto, com senha específica, e permitir o envio de traps SNMP ao CONTRATANTE ou seu preposto.
- 3.6. A CONTRATADA deverá permitir acesso à leitura da configuração dos roteadores, pelo CONTRATANTE ou seu preposto, através de usuário e senha específicos.
- 3.7. A configuração lógica dos roteadores será definida pela CONTRATADA com a aprovação da CONTRATANTE.
- 3.8. A CONTRATADA deverá dimensionar o tipo e a quantidade de roteadores dos sites remotos, aqueles que farão parte do link CPD - sites remotos, além dos roteadores do site principal e secundário do CONTRATANTE em Belém/PA.
- 3.9. Todos os roteadores deverão possuir interface para conexão com modem assíncrono ou possibilitar a instalação de modem interno nestes equipamentos.
- 3.10. O CONTRATANTE disponibilizará uma linha telefônica a fim de prover manutenção remota nos roteadores via acesso discado, quando se fizer necessário.
- 3.11. A CONTRATADA será responsável pela devida instalação, configuração e manutenção dos roteadores, por ela alocados, a fim de garantir o pleno funcionamento da rede.
- 3.12. Os roteadores a serem disponibilizado pela CONTRATADA para o sites central (Primário) e Secundário (Backup) deverão atender aos seguintes requisitos:
 - a) Os CPE devem possuir no mínimo 2 (duas) interfaces LAN: IEEE 802.3, 802.3u e 802.3ab – Especificação 10/100/1000BASE-T (Full Duplex) RJ-45 para a interconexão com a rede local do CONTRATANTE;
 - b) Suportar o padrão IEEE 802.1q, de forma a permitir a conectividade de diversas LANs a partir de um único roteador CPE;
 - c) Implementar VAD (Voice Activity Detection) para quaisquer taxas de transmissão e cRTP (compressão de cabeçalho RTP) para taxas de transmissão inferiores a 512 kbps;
 - d) Implementar os protocolos de voz (VoIP) H.323 v2 e SIP;
 - e) A CONTRATADA deverá configurar os recursos roteadores CPE, controlador de chamadas (gateway keeper) e dentre outros com o protocolo SIP para o provimento do serviço de interligação dos PABXs, como por entroncamentos E1 para interconexão com o PABX do CONTRATANTE.
 - f) Implementar o serviço de voz com suporte aos padrões de compressão de voz ITU-T: G.729, G711 e T38;
 - g) Implementar os protocolos de roteamento com autenticação: RIPv2 (RFC 2453), OSPF (RFC 1583);

- h) Implementar o protocolo BGPv4 conforme RFCs 1771;
 - i) Suportar mecanismos de escalonamento de filas que permitam a reserva de largura de banda mínima para cada fila. Deverá ser suportado um valor mínimo de 24 filas;
 - j) Suportar capacidade de filtros de pacotes (por protocolo, endereço IP de origem, endereço IP de destino, porta de UDP/TCP de origem, porta de UDP/TCP de destino);
 - k) Suportar capacidade de gerenciamento através de SNMP compatível com versões V.2 e V.3.
 - l) Suportar MIB-II e RMON;
 - m) Suportar servidor DHCP de acordo com a RFC 2131 (Dynamic Host Configuration Protocol) permitindo a atribuição de endereços IP a estações a partir do roteador e permitindo definir o endereço IP de acordo com o MAC address de cada equipamento;
 - n) Suportar "BOOTP relay agents" de acordo com a RFC 2131 (Dynamic Host Configuration Protocol) permitindo a atribuição de endereços IP a estações localizadas na rede local a partir de um servidor DHCP localizado em uma rede remota;
 - o) Implementar sincronismo via protocolo NTP (Network Time Protocol) com autenticação (RFC 1305);
- 3.13.** Os roteadores a serem disponibilizados pela CONTRATADA para os sites remotos devem atender aos seguintes requisitos:
- a) Os roteadores devem possuir no mínimo 2 (duas) interfaces LAN: IEEE 802.3 e 802.3u – Especificação 10BASE-T e 100BASE-Tx (Full Duplex), com conector do tipo RJ-45;
 - b) Implementar VAD (Voice Activity Detection) para quaisquer taxas de transmissão e cRTP (compressão de cabeçalho RTP) para taxas de transmissão inferiores a 512 kbps;
 - c) Implementar os protocolos de voz (VoIP) H.323 v2 e SIP;
 - d) A CONTRATADA deverá configurar os recursos (roteadores CPE, controlador de chamadas, dentre outros) com o protocolo SIP para o provimento do serviço de interligação dos aparelhos telefônicos e PABX, quando solicitado pelo CONTRATANTE;
 - e) Implementar o serviço de voz com suporte aos padrões de compressão ITU-T: G.729, G711 e T38;
 - f) Os roteadores deverão obrigatoriamente vir equipados com no mínimo 4 interfaces analógicas, que estão definidas no A
 - g) nexa II;
 - h) Implementar os protocolos de roteamento: RIPv2 (RFC 12453) e OSPF (RFC 1583);
 - i) Suportar mecanismos de escalonamento de filas que permitam a reserva de largura de banda mínima para cada fila. Deverá ser suportado um valor mínimo de 12 filas;
 - j) Suportar capacidade de gerenciamento através de SNMP compatível com versões v2c e v3.
 - k) Suportar MIB-II e RMON;

- l) Suportar servidor DHCP de acordo com a RFC 2131 (Dynamic Host Configuration Protocol) permitindo a atribuição de endereços IP a estações a partir do roteador e permitindo definir o endereço IP de acordo com o MAC address de cada equipamento;
- m) Suportar "BOOTP relay agents" de acordo com a RFC 2131 (Dynamic Host Configuration Protocol) permitindo a atribuição de endereços IP a estações localizadas na rede local a partir de um servidor DHCP localizado em uma rede remota;
- n) Implementar sincronismo via protocolo NTP (Network Time Protocol) com autenticação (RFC 1305).

3.14. Todos os roteadores CPE a serem disponibilizados pela CONTRATADA devem suportar QoS e atender aos seguintes requisitos.

- a) Suportar classificação de tráfego de acordo com diversos critérios (interface, IP origem/destino, portas TCP/UDP, dentre outros) em cada interface física e lógica (sub-interfaces);
- b) Implementar QoS conforme arquitetura "Differentiated Services" (RFCs 2474, 2475);
- c) Implementar LFI (Link Fragmentation and Interleaving) nas interfaces seriais com encapsulamento PPP;
- d) Implementar MLPPP (multilink PPP) nas interfaces seriais;
- e) "Traffic Shaping" genérico (independente da tecnologia de transporte nível 2);
- f) Permitir métodos de priorização de tráfego (QoS) por tipo de protocolo e por serviços da pilha TCP/IP além de "Traffic Policing" e "Traffic Shaping": Priority Queuing, Class Based Queuing (CBQ), Generic Traffic Shaping (GTS);
- g) Implementar classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point);
- h) Implementar WRED (Weighted Random Early Detection);
- i) Possibilidades de definição de classes de serviço e alocação de banda por classes nas interfaces do equipamento. Para os pacotes que excederem a especificação de banda deve ser possível configurar pelo menos as seguintes ações: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote. Deve ser possível criar uma classe com prioridade absoluta sobre as demais dentro da quantidade de banda que lhe foi alocada;
- j) Deve implementar os seguintes recursos de QoS: Policy Routing, WFQ (Weighted Fair Queuing), LLQ (Low Latency Queue), GTS (Generic traffic shaping), e DSCP (Differentiated services control point);
- k) Classificação e marcação de tráfego baseadas no campo CoS ("Class of Service") de frames Ethernet, conforme definição do padrão IEEE 802.1p;
- l) Compressão do cabeçalho dos pacotes RTP para otimização da transmissão de pacotes de VoIP (Voz sobre IP).

3.15. Gerência/administração

- a) Protocolo TACACS com suporte integral à arquitetura AAA (Authentication, Authorization, Accounting), sendo possível especificar os grupos de comandos de configuração/monitorização permitidos a cada grupo de usuários. Devem ficar registradas no servidor AAA todos os comandos executados pelos usuários autorizados assim como todas as tentativas não autorizadas de execução de comandos nos equipamentos;



- b) Acesso SSH com algoritmo de criptografia com chave de pelo menos 168 bits (3 DES);
- c) SNMPv1, SNMPv2 e SNMPv3, com possibilidades de definição da interface de origem dos pacotes SNMP.
- d) Pelo menos 02 grupos de RMON (eventos e alarmes);
- e) NTP (Network Time Protocol) com autenticação entre os peers (RFC 1305), possibilidade de definição da interface de origem dos pacotes NTP e NTP por VRF.

3.16. Segurança

- a) Disponibilizar, no mínimo, 02 (dois) níveis de senha de acesso com privilégios de leitura;
- b) Disponibilizar controle das sessões telnet – possibilidade de filtrar os endereços IP específicos autorizados a executar sessão telnet com o roteador (configuração de login);
- c) Implementar criptografia 3DES (ou superior) para os acessos SSH;
- d) Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP (e UDP), status dos flags “ACK”, “SYN” e “FIN”;
- e) Deve suportar mecanismo de tunelamento VPN com IPSec, GRE, L2TP e L2F;
- f) Deve suportar criação de VPNs através do conjunto de especificações IPSEC. Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409. Devem ser suportados no mínimo os algoritmos DES (56 bits), 3DES (168 bits), AES-128 e AES-256 para garantia de confidencialidade às conexões IPSEC;
- g) O equipamento fornecido deve suportar no mínimo uma IPSEC do tipo “site-to-site”. Suporte a certificados digitais para autenticação das conexões IKE. Possuir mecanismo de automatização do processo de enrollment na autoridade certificadora para no mínimo as seguintes CAs de mercado: Entrust, Verisign, Microsoft e RSA.

LOTE 02

4. REDE DE ALTA VELOCIDADE

- 4.1.** A CONTRATADA deverá fornecer circuitos de alta velocidade para contingência e replicação do banco de dados entre os sites Primário e Secundário da CONTRATANTE, utilizado acessos de fibra óptica em anel e interfaces Fibre Channel (FC) e Giga Ethernet (GE) a serem prontamente utilizados em caso de desastre/falhas no site principal.
- 4.2.** A CONTRATADA deverá fornecer circuitos de alta velocidade dedicados através de uma solução escalável utilizando a tecnologia de rede DWDM.
- 4.3.** A CONTRATADA deverá garantir um tempo médio de desempenho mensal de latência para enlaces terrestre menor que 5ms.
- 4.4.** O meio físico de acesso dos circuitos concentradores (Primário e Secundário), por questões de qualidade e escalabilidade e disponibilidade, deve ser fornecido por meio de fibra óptica em anel com contingência automática, garantindo assim a continuidade da prestação do serviço em caso de interrupção em um dos segmentos do acesso.

- 4.5. A CONTRATADA deverá disponibilizar a infraestrutura necessária de acesso para atender às necessidades de comunicação de dados do CONTRATANTE.
- 4.6. A relação de endereços dos pontos de acesso à rede, com as respectivas especificações de larguras de banda e outras características é apresentada **Parágrafo Terceiro da Cláusula Terceira** deste Contrato.
- 4.7. A **CONTRATADA** deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados.
- 4.8. O CONTRATANTE terá o direito de verificar a correta aplicação dessas políticas, através da realização de auditorias periódicas remotas e in-loco, dos ambientes físicos e lógicos da CONTRATADA.
- 4.9. Essa ação tem como intuito a prevenção de incidentes de segurança para garantir os níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do CONTRATANTE.
- 4.10. As velocidades de transmissão para os 04 (quatro) circuitos FIBRE CHANNEL serão de 8 GIGABIT/S;
- 4.11. As velocidades de transmissão para os 04 (quatro) circuitos GIGAETHERNET serão de 40 GIGABIT/S;
- 4.12. As dependências do CONTRATANTE deverão dispor de infraestrutura necessária, incluindo espaço, energia, climatização, tubulações para passagem de cabos, rack e equipamentos necessários para receber os circuitos de alta velocidade;
- 4.13. O CONTRATANTE deverá permitir a entrada dos técnicos da CONTRATADA e seus terceirizados para realizarem a implantação do serviço proposto;
- 4.14. A solução contempla a instalação nos sites do cliente de 02 (dois) sistemas DWDM, um para cada rota física, com comutação automática em caso de falha em uma das rotas ou em um dos equipamentos associado a uma das rotas;
- 4.15. Serão disponibilizadas as interfaces FIBRE CHANNEL e GIGAETHERNET (1000 base-T) nos equipamentos de replicação, para o lado do cliente.
- 4.16. No caso de necessidade futura do CONTRATANTE em expandir os circuitos de alta velocidade até o limite de 08 (oito) circuitos FIBRE CHANNEL de 08 (oito) GIGABIT/S, serão utilizados como referência para efeito de cálculo, os valores unitários das velocidades requeridas pelo CONTRATANTE, conforme planilha deste Contrato.

LOTE 03

5. CONECTIVIDADE A REDE INTERNET

- 5.1. A CONTRATADA deverá fornecer circuitos com conectividade direta com a rede Internet através de acessos dedicados em fibra óptica em anel redundantes e portas IP exclusivas como fornecimento total de conectividade IP (Internet Protocol) com suporte à aplicações TCP/IP.
- 5.2. A CONTRATADA deverá prover o acesso direto à Internet, de forma não compartilhada, devendo estar disponível 24 (vinte e quatro) horas por dia, durante os 07 (sete) dias da semana, e constituir-se de acessos permanentes, dedicados, e com total conectividade IP, interligando a CONTRATADA à Internet, através de canais privativos que possuam redundância de rota.

- 5.3.** A CONTRATADA deverá disponibilizar a infraestrutura necessária (hardware, software, roteadores, acesso, porta) suportada por rede terrestre e circuitos dedicados.
- 5.4.** Os roteadores fornecidos pela CONTRATADA que atenderão os circuitos de Internet deverão, obrigatoriamente, estar de acordo com as especificações solicitadas no item 4.12.
- 5.5.** O Backbone da CONTRATADA deverá ter garantia de desempenho e suporte a diversos protocolos e permitir a utilização de endereçamento IP público.
- 5.6.** A CONTRATADA deverá oferecer ferramentas para a emissão de relatórios diários sobre o tráfego escoado pela rede com suas séries históricas, de forma que a CONTRATANTE possa analisar o desempenho e as tendências de utilização de recursos de rede utilizados pelas suas aplicações. O acesso aos relatórios deverá ser disponibilizado via Internet e utilizar "browser" padrões de mercado, como Internet.
- 5.7.** A CONTRATADA deverá disponibilizar uma solução de Gerência de Rede e Serviços abrangendo todo o serviço prestado e contemplando as áreas funcionais de gerência de Falhas, Desempenho, Configuração e de Nível de Serviço.
- 5.8.** A CONTRATADA deverá Disponibilizar conectividade com rede INTERNET através do fornecimento de dispositivos que garantam a segurança e proteção da porta WAN (proteção contra ataques de negação de serviços, evitando assim a saturação da banda de internet e indisponibilidade dos serviços em momentos de ataques DOS e DDOS.) no backbone da CONTRATADA.
- 5.9.** A CONTRATADA fornecerá uma conexão dedicada por rede de fibra óptica em anel com contingência automática de forma dedicada e exclusiva (não compartilhado) com o estabelecimento de 02 (dois) circuitos ponto a ponto, entre seu backbone Internet e o backbone da CONTRATANTE através de circuitos de acesso local, nas velocidades de 500 Mbps cada.
- 5.10.** A CONTRATADA deverá prover e manter, o meio físico e os equipamentos necessários (fibra óptica e roteador) para a interligação do seu backbone Internet, incluindo as interfaces físicas, com o backbone da rede da CONTRATANTE.
- 5.11.** A instalação de ponto de acesso físico deverá ser entregue na sala destinada para esse fim, nas dependências da CONTRATANTE.
- 5.12.** O protocolo de transporte entre o roteador da CONTRATANTE e o roteador do backbone da CONTRATADA deverá ser ETHERNET.
- 5.13.** A CONTRATADA deverá oferecer transição facilitada para o serviço de IP hoje disponível na CONTRATANTE, visto que esta nova contratação poderá, ou não, resultar na manutenção do direcionamento dos Servidores de DNS hoje existentes, atrelados ao endereço IP classe C junto à FAPESP.
- 5.14.** A CONTRATADA deverá atribuir à rede da CONTRATANTE, 256 endereços IP de (uma) classe tipo C válidos na Internet, derivados do bloco CIDR (Classless Inter-Domain Routing) alocado ao seu backbone. Esta atribuição deverá seguir as orientações do IAB (Internet Activities Board).
- 5.15.** A CONTRATADA deverá fornecer o serviço de DNS secundário, para uso por parte da CONTRATANTE.
- 5.16.** A CONTRATADA deverá oferecer conexão através de interface física FastEthernet ou GigaEthernet, através de roteador próprio com suporte a Firewall, cabendo-lhe a responsabilidade pela configuração e manutenção do referido equipamento.

- 5.17.** À CONTRATADA caberá o dimensionamento, fornecimento, instalação e manutenção dos roteadores exclusivos e independentes dos roteadores da Rede IP Multiserviços, localizados na CONTRATANTE, para os serviços supracitados.
- 5.18.** A CONTRATADA deverá garantir um tempo médio de desempenho mensal de latência, no núcleo da rede, de no máximo 150 ms (milessegundos), comprovados através de relatórios estatísticos de acompanhamento via portal Web. A latência é o tempo que um pacote IP leva para ir e voltar (round-trip) de um ponto a outra da Rede.
- 5.19.** A Média Mensal de Perda de Pacotes no núcleo da rede da CONTRATADA, não deverá ultrapassar ao valor máximo de 2%, comprovados através de relatórios estatísticos de acompanhamento diário via portal Web. Chamamos Perda de Pacotes o índice que mede a taxa de sucesso na transmissão de pacotes IP entre dois pontos da Rede.
- 5.20.** A Disponibilidade Média Mensal no núcleo da rede da CONTRATADA deverá ser igual ou superior a 99,7%, comprovados através de relatórios estatísticos de acompanhamento diário via portal Web. Entende-se por Disponibilidade Média Mensal do núcleo da rede o índice que mede o tempo que uma rede esteve operacional para transmissão e recepção de pacotes IP.
- 5.21.** No cálculo da disponibilidade, serão consideradas todas as interrupções, exceto as programadas. A CONTRATADA deverá garantir os índices de desempenho usados como referência para garantia de nível de serviço (SLA) tomando como base a latência média mensal de 150 ms, perda de pacotes média mensal de 2 % e disponibilidade média mensal de 99,7 %.
- 5.22.** À CONTRATADA deverá prover gerência pró-ativa da porta IP, a qual consiste em monitorar a porta do roteador da CONTRATANTE, efetuando a verificação automática da disponibilidade do link de, no máximo, a cada 05 (cinco) minutos, caso o roteador da CONTRATANTE não responda após 03 (três) tentativas, deverá ser disparado procedimentos de correção e a CONTRATANTE deverá ser avisada em até 30 minutos.
- 5.23.** À CONTRATADA caberá fornecer os equipamentos necessários a prestação do serviço como modem's, roteadores para integração à rede local da CONTRATANTE, acesso em fibra óptica sendo responsável pela devida instalação e manutenção, a fim de garantir o pleno funcionamento da rede.
- 5.24.** A CONTRATADA será responsável pela dimensionamento dos equipamentos, instalação, configuração, manutenção dos roteadores e equipamentos, por ela alocados, a fim de garantir o pleno funcionamento da conectividade com a rede Internet.
- 5.25.** O site central deve obrigatoriamente ser atendido por fibra em anel com redundância automática, sendo que os acessos do anel devem ser realizados por caminhos distintos até o ponto de presença (POP) da CONTRATADA.
- 5.26.** A unidade principal e secundária deverão utilizar roteadores CPE distintos com balanceamento automático de carga entre eles;
Os acessos da unidade principal e secundário deverão estar interligados diretamente aos roteadores de borda distintos da CONTRATADA, obedecendo aos requisitos abaixo:
- a) Na solução de contingência, deverão ser disponibilizados dois roteadores interconectados um ao outro através de conexão Fast ou Giga Ethernet, conectados a cada um dos enlaces, operando com protocolo de redundância e operando com balanceamento automático de tráfego (exemplo: GLBP – *Gateway Load Balancing Protocol*, BGP – *Border Gateway Protocol*);



- b) Na ocorrência de falha ou intermitência no funcionamento de um roteador CPE, a contingência deverá ser acionada automaticamente e proteger o tráfego que era cursado pelo(s) elemento(s) em falha em até 5 segundos.
 - c) Após a solução da falha causadora do contingenciamento o tráfego deverá retornar automática e imediatamente para a situação anterior à falha.
- 5.27.** A CONTRATADA deve possuir centro de Roteamento Internet (roteador de Backbone) na cidade de Belém/PA com saída de backbone terrestre desta capital para o backbone nacional da rede Internet com no mínimo, o somatório de banda de 5 Gbps.
- 5.28.** A CONTRATADA deverá seguir as determinações do órgão regulador de Internet brasileiro no que tange a implementação e uso do protocolo IPV6, sendo obrigatório a implementação deste protocolo no momento que o órgão regulador determinar seu uso.
- 5.29.** A CONTRATADA deverá estar preparada para fornecer conectividade IPV6, conforme plano de migração do CONTRATANTE, obedecendo prazos acordados previamente entre as partes e sem ônus de qualquer natureza.
- 5.30.** A CONTRATADA deverá apresentar declaração e/ou Anotação de Responsabilidade Técnica de expedida pelo CREA de qualquer unidade da federação, que dispõe de circuitos exclusivos com o exterior, de no mínimo 5 (cinco) Gbps (Gigabits por segundo), correspondendo a somatória de banda de todos os circuitos. Essa saída deve ser composta por uma ou mais conexões ponto-a-ponto entre o backbone IP do provedor e do sistema autônomo (AS-Autonomous System) remoto, sem backbones intermediários (em caso de apresentação de declaração, o CONTRATANTE realizará diligência em qualquer tempo e hora para comprovação técnica referente a exigência deste item);
- 5.31.** A CONTRATADA deverá comprovar através de declaração e/ou Anotação de Responsabilidade Técnica de expedida pelo CREA de qualquer unidade da federação, que pode se conectar com no mínimo, 4 (quatro) AS/provedores diferentes dos Estados Unidos da América (EUA) (em caso de apresentação de declaração, o Banco da Amazônia realizará diligência em qualquer tempo e hora para comprovação técnica referente a exigência deste item);
- 5.32.** A CONTRATADA deverá comprovar através de declaração e/ou Anotação de Responsabilidade Técnica de expedida pelo CREA de qualquer unidade da federação, que o backbone IP da PARTICIPANTE deverá possuir saída com destino a outros provedores de backbone IP Nacionais, com banda mínima de 5 (cinco) Gbps (em caso de apresentação de declaração, o Banco da Amazônia realizará diligência em qualquer tempo e hora para comprovação técnica referente a exigência deste item);
- 5.33.** A CONTRATADA deverá comprovar através de declaração e/ou Anotação de Responsabilidade Técnica de expedida pelo CREA de qualquer unidade da federação, que o backbone IP do provedor deve ser capaz de prover trânsito nacional e internacional para o SISTEMA AUTÔNOMO (AS) do BANCO DA AMAZÔNIA, com suporte ao protocolo BGP-4 (em caso de apresentação de declaração, o Banco da Amazônia realizará diligência em qualquer tempo e hora para comprovação técnica referente a exigência deste item);
- 5.34.** A CONTRATADA deverá fazer o dimensionamento para os sites centrais (Primário e Secundário) para fornecer os equipamentos com capacidade adequadas considerando a quantidades de conexões simultâneas de tráfego gerando considerando como requisitos mínimos as especificações exigidas nos itens 6.36, 6.37 e 6.38.

5.35. A CONTRATADA deverá disponibilizar em seu backbone proteção contra ataques de negação de serviços, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DOS e DDOS de acordo considerando os requisitos mínimos a seguir:

- 5.35.1. Serviços deverão ter pró-atividade para solução e prevenção de incidentes e ataques;
- 5.35.2. Monitorar disponibilidade e performance de todos os links de dados existentes nesse termo de referência em regime 24x7 utilizando profissionais de forma dedicada;
- 5.35.3. Tomar todas as providências necessárias para recompor a disponibilidade do link em caso de incidentes de ataques de DDoS, recuperando o pleno funcionamento do mesmo pela contratada.
- 5.35.4. A solução deve possuir a capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.
- 5.35.5. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.
- 5.35.6. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, incluindo, mas não se restringindo aos seguintes:
 - Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;
 - Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;
 - Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;
 - Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);
 - Ataques à camada de aplicação, incluindo protocolos HTTP e DNS.
- 5.35.7. A solução deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA.
- 5.35.8. A CONTRATADA deve possuir dois centros de limpeza nacional cada um com capacidade mínima de mitigação de 1GB, centro de limpeza internacional com capacidade mínima de mitigação de 30GB.
- 5.35.9. A contratada deve mitigar ataques por 3 horas, caso o ataque ultrapasse o SLA de mitigação contratado.
- 5.35.10. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole,



- 5.35.11. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.
- 5.35.12. A CONTRATADA deve disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.
- 5.35.13. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.
- 5.35.14. Em momentos de ataques DOS e DDOS, todo tráfego limpo deve ser reinjetado na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante.
- 5.35.15. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.
- 5.35.16. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual
- 5.35.17. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada.
- 5.35.18. A contratada deve possuir um contrato de 15 minutos para iniciar a mitigação de ataques de DDOS
- 5.35.19. A **CONTRATADA** deverá disponibilizar uma Solução de Monitoração de acompanhamento contra ataques DDoS, que contemple:
- a) Quadro Sinóptico para visualização da ocupação de banda do link Internet e níveis de severidade dos ataques.
 - b) Os alertas, que deverão fornecer, no mínimo, as seguintes funcionalidades:
 - Visualização de informações on-line, de forma gráfica da banda consumida no ataque;
 - Acompanhamento do nível de importância do ataque, o percentual do nível de severidade do ataque, o consumo de banda do ataque e tipo do ataque e classificação.
 - Origem de ataques com identificação do endereço IP e porta de origem

- Destino de ataques, com identificação do endereço IP e porta de destino.
- Protocolo de transporte do alerta.
- Cada alerta deverá ter um numero de identificação que facilite sua consulta.
- Informar a data de inicio e fim do acompanhamento do alerta
- Volume de ataques sumarizados por hora, dia, semana e mês.
- Relatório por tipos de ataques.

c) O Portal de monitoração da CONTRATADA deverá possuir uma interface única para acesso às suas funcionalidades, independentemente dos equipamentos ou tecnologias empregadas para a prestação dos serviços.

d) O Portal de Gerência deverá permitir o acesso simultâneo a, pelo menos, um administrador de rede da CONTRATANTE.

5.36. A CONTRATADA deverá comprovar através de declaração e/ou Anotação de Responsabilidade Técnica de expedida pelo CREA de qualquer unidade da federação, que possui no seu o backbone IP serviço de limpeza contra ataques DDOS (Distributed Denial of Service) em cliente que possuam com conexão a Internet de no mínimo 100 Mb ou superiores e com mitigação contra ataques de no mínimo 1Gb para ataques nacionais e 30 Gb contra ataques internacionais, compatíveis e pertinentes com o objeto desta licitação.

5.37. A CONTRATADA deverá oferecer serviço de transição dos IP hoje disponíveis e em uso no CONTRATANTE para utilização do AS (Autonomous System) do CONTRATANTE.

5.38. O CONTRATANTE poderá solicitar a desativação do serviço prestado de acordo com Lei.

ANEXO VII**ACORDO DE NIVEIS DE SERVIÇO E INTERRUPÇÃO DE SERVIÇO****1. SLA (Service Level Agreement)**

- 1.1.** Latência consiste no tempo médio de trânsito (ida e volta – round-trip delay) de um pacote de 64 bytes entre dois pontos distintos da rede do CONTRATANTE, onde a mesma poderá solicitar, a qualquer momento, em quais sites será feita a medição.

1.1.1. O tempo de resposta, medido através de pacotes ICMP de 64 bytes deverá ser igual ou inferior a 650 ms enlases que usem comunicação via satélite SCPC, e igual e inferior a 150ms para enlases terrestres.

1.1.2. Quando os acessos solicitados para medição forem um terrestre e outro satélite dedicado, o tempo de resposta medido através de pacotes ICMP de 64 bytes deverá ser igual ou inferior a 800 ms.

- 1.2.** A Taxa de Perda de Pacotes será determinada testando-se a Rede de Comunicação Digital desde a porta WAN (Wide Area Network) do roteador baseado no CONTRATANTE (ponta A), até a porta WAN respectiva do roteador de uma unidade remota da rede (ponta B). De cada 100 (cem) pacotes, a perda máxima permitida é de 2% (dois por cento).

1.2.1. Será admitido taxa de erros (BER), igual ou superior a 10^{-6} para acesso terrestre e 10^{-8} para acesso satélite.

- 1.3.** Disponibilidade do Serviço de Comunicação Digital é o índice que mede o percentual de tempo que uma unidade específica da Rede (ponto de acesso integrante do serviço) esteve operacional para transmissão e recepção (condições normais de funcionamento e operação), no período de 01 (um) mês.

a) Para o site central a disponibilidade mínima deve ser de 99,7 %, equivalente a um máximo de 02h09min parados por mês.

b) Para os sites remotos atendidos nas capitais a disponibilidade mínima deve ser de 99,4%, equivalente a um máximo de 04h19min parados por mês.

c) Para os sites remotos atendidos no interior dos Estados a disponibilidade mínima deve ser de 99,3 %, equivalente a um máximo de 06h00min parados por mês.

- 1.4.** O serviço será considerado indisponível:

1.4.1. A partir do início de uma interrupção ou instabilidade recorrente (intermitência) registrada de forma automática no sistema de gerência da CONTRATADA, pelo registro automático no sistema de monitoração do CONTRATANTE ou registro na Central de Assistência Técnica (Call Center) da CONTRATADA até o total restabelecimento do circuito às condições normais de operação e a respectiva informação e certificação pelo CONTRATANTE.

- 1.5.** A disponibilidade do serviço será calculada, por cada ponto de acesso à rede, para um período de 1 mês, através da seguinte equação:

$D = \frac{T - T_i}{T_0} \times 100$ Onde:	D = disponibilidade; T₀ = período de operação (1 mês), em minutos; T_i = tempo total de indisponibilidade do ponto de acesso, ocorrida no período de operação (1 mês), em minutos.
---	--

- 1.6.** No cálculo de disponibilidade, não serão consideradas as interrupções programadas, as de urgência e aquelas que não sejam de responsabilidade da CONTRATADA.

1.6.1. Considera-se paralisação programada da CONTRATADA a interrupção para manutenção preventiva ou para substituição dos equipamentos e meios utilizados no provimento do serviço, desde que devidamente informados com antecedência mínima de 5 (cinco) dias úteis, não podendo ultrapassar os seguintes limites por circuito:

- a) Tempo máximo da interrupção: Até 180 (cento e oitenta) minutos por circuito. Caso esse prazo venha a ser ultrapassado, o mesmo deve ser previamente comunicado ao CONTRATANTE.
- b) Frequência máxima a 1 (uma) ocorrência em cada 30 (trinta) dias, não acumulativo.
- c) Quando for necessária ação da CONTRATADA nas dependências do CONTRATANTE ou de seus clientes, deverá ser solicitado prévio acesso ao preposto do contrato ou quem ele designar.
- d) Quando o prazo mínimo de 5 (cinco) dias úteis de comunicação não for atendido, ou não houver a informação registrada, a interrupção incidirá no cômputo do cálculo de indisponibilidade do serviço.

1.7. Considera-se paralisação de urgência pela CONTRATADA a interrupção para manutenção preventiva ou para substituição dos equipamentos e meios utilizados no provimento do serviço que comprovadamente comprometam o seu funcionamento mediante índices de degradação do circuito (banda passante, tempo de resposta e taxa de erro). Devendo, entretanto, ser comunicado ao CONTRATANTE até 2 (duas) horas antes do início do atendimento através de relatório, para ciência do corpo técnico do CONTRATANTE. Caso contrário, a interrupção incidirá no cômputo do cálculo de indisponibilidade do serviço a ser aplicado pelo CONTRATANTE.

1.8. Considera-se paralisação como não sendo responsabilidade da CONTRATADA os eventos relacionados à ocorrência de caso fortuito (entende-se como caso fortuito como sendo qualquer ocorrência que não seja proveniente de qualquer ação humana, tais como: descargas atmosféricas, tremores de terra, maremotos, enchentes, etc.) ou que venham a ser causados por qualquer ação dos clientes do CONTRATANTE ou do próprio CONTRATANTE, bem como falhas em seus equipamentos.

1.9. Quando os valores de disponibilidade estabelecidos para os Serviços não forem atendidos pela CONTRATADA, será concedido ao CONTRATANTE um desconto por interrupção, conforme o item 2.8.

2. INTERRUÇÃO DE SERVIÇO

2.1. Caso haja interrupções não programadas ou de urgência nos serviços, a CONTRATADA fica sujeita a pagamento das multas, da seguinte forma:

2.1.1. A CONTRATADA realizará o pagamento das multas por interrupção no funcionamento do(s) acesso(s) no mês subsequente à prestação do serviço, cujas causas não sejam atribuídas ao CONTRATANTE, observadas as demais condições estabelecidas no contrato.

2.2. Para efeito de descontos, o tempo de interrupção deverá ser considerado entre o início da interrupção registrada na gerência/supervisão do CONTRATADA ou a partir da comunicação de interrupção, feita pelo CONTRATANTE, e a sua total recuperação, após informação ao CONTRATANTE.

2.3. Para efeito de desconto, o período mínimo a ser considerado é de 30 (trinta) minutos consecutivos, adotando-se como início da contagem o tempo e o horário da ocorrência do fato que proporcionou o CONTRATANTE o direito de receber o desconto.



- 2.4.** Os períodos adicionais serão considerados como períodos inteiros de 30 (trinta) minutos.
- 2.5.** O valor do desconto será aplicado no mês imediatamente subsequente ao mês no qual ocorreram os fatos que originaram os descontos, tendo como base o valor vigente do(s) acesso(s) do mês da ocorrência da interrupção.
- 2.6.** Não serão concedidos descontos por interrupção, na ocorrência de evento ocasionado por operação inadequada por parte do CONTRATANTE, por falha na infraestrutura do CONTRATANTE e por falhas na rede elétrica interna ou externa.
- 2.7.** A CONTRATADA não ficará sujeita às multas em caso de paralisações programadas, de urgência e que não sejam de responsabilidade da CONTRATADA, conforme itens 18.2 do TR.
- 2.8.** O valor do desconto a ser concedida a CONTRATADA será obtido através do seguinte cálculo:

$VD = \frac{VM}{1440} \times N$ Onde:	VD= Valor do Desconto; VM = Valor Mensal do Circuito N = Quantidade de unidades de períodos de 30 (trinta) minutos em que o Serviço ficou interrompido.
--	--

- 2.9.** A CONTRATADA deverá prestar suporte operacional ao Banco em todas as localidades onde houver Agência, Superintendência ou Posto, através de sua equipe técnica.
- 2.10.** Em situações de falhas na comunicação por deficiência em equipamentos ou por outro motivo de responsabilidade da CONTRATADA, o Banco cobrará multa que incidirá sobre a fatura mensal daquele mês, o pagamento da multa por interrupção no funcionamento do(s) acesso(s) será em depósito na conta corrente a ser informado pelo CONTRATANTE sendo igual a 05 (cinco) dias de prestação do serviço para cada dia de paralisação do circuito, calculado “pro-rata die”. O tempo de interrupção a ser cobrado independe dos prazos definidos para tempo de atendimento e recuperação os quais serão acordados no item 15-Garantia e Assistência Técnica, limitado a 10% do valor mensal do contrato.
- 2.11.** O CONTRATANTE fará mensalmente a contabilização das multas e descontos e encaminhará a CONTRATADA para aferição e contestação no mês em questão, podendo a CONTRATADA realizar apenas uma contestação do mês avaliado. Após o aceite do mês analisado a CONTRATADA não poderá fazer nova contestação, devendo proceder com os pagamentos das multas e descontos.
- 2.12.** Neste Anexo está descrita proposta de planilha de acompanhamento de SLA.

3. MULTAS E PENALIDADES PARA O ACORDO DE NÍVEL DE SERVIÇOS – SLA

- 3.1.** Pelo não cumprimento do SLA (Acordo de níveis de serviço) por chamado o CONTRATANTE poderá, garantido o contraditório e a ampla defesa, sem prejuízo das demais cominações previstas neste Contrato, aplicar as multa e penalidades previstas nas Leis Nº 10.303/2016, 10.520/2002 e no Decreto nº 5.450/2005:

Classificação	Descrição	Multa/Penalidade
Muito Alto	Indisponibilidade ou degradação das Funções Vitais da Solução	Multa de 1% (dez por cento) sobre o valor global do lote na
Classificação	Descrição	Multa/Penalidade
Alto	Indisponibilidade ou degradação de Funções Não vitais da Solução, porém de alta	Multa de 0,5% (dez por cento) sobre o valor global do lote na contratação.
Média	Indisponibilidade ou degradação das Funções Não vitais da Solução	Multa de 0,3% (um por cento) sobre o valor global do lote na contratação.
Baixa	Chamados de impacto nulo ou baixo da Solução	Advertência ou Multa de 0,1% (um por cento) sobre o valor global do lote na contratação.

- 3.2. As multas e penalidades poderão ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório, e a sua cobrança não isentará da obrigação de indenizar eventuais perdas e danos.
- 3.3. Nenhuma multa ou penalidade será aplicada pelo CONTRATANTE sem o devido processo administrativo, assegurado o contraditório e a ampla defesa, no prazo de 5 (cinco) dias úteis, a partir da notificação do CONTRATANTE.
- 3.4. Após o devido processo administrativo, sendo constatada a responsabilidade da parte contrária pelo não cumprimento do SLA, o valor das multas será descontado pelo CONTRATANTE do valor da garantia, da fatura mensal devido, cobrado diretamente da contratada ou judicialmente:
- 3.5. Se a multa for valor superior ao valor da garantia apresentada, além da perda desta, responderá a Parte contrária pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pelo CONTRATANTE.
- 3.6. Inexistindo pagamento devido pela CONTRATADA, ou sendo este insuficiente, caberá a parte contrária efetuar o pagamento do que for devido, no prazo máximo de 10 (dez) dias consecutivos, contados da data de sua comunicação de confirmação da multa, em depósito em conta corrente própria em nome do CONTRATANTE.
- 3.7. No caso de não adequação às instruções contidas nos normativos publicados pelo CONTRATANTE, passado o período de carência de 30(trinta) dias, incidirá multa sobre o valor total do contrato, da ordem de 0,2% (dois décimos por cento) ao dia, sobre cada item, alínea ou tema não conforme.
- 3.8. O descumprimento dos prazos previstos relativo à execução dos serviços, bem como pela não realização de ações de contingência que garantirão a continuidade dos serviços, durante o período de garantia, implicará na cobrança de multa de 3% (três por cento) ao dia.
- 3.9. Caso não seja garantido absoluto sigilo sobre todos os processos, rotinas, objetos, informações, documentos e quaisquer outros dados fornecidos pelo CONTRATANTE, implicará na cobrança de multa compensatória correspondente a 5% sobre o valor total do contrato, além das cominações previstas na Legislação, podendo o CONTRATANTE rescindir o presente contrato.
- 3.10. Na forma dos parágrafos 2º e 3º do art. 86 da Lei 10.303/16, as multas contratuais acima dispostas serão descontadas da garantia do contrato, após regular processo administrativo. Em caso de multa superior ao valor da garantia prestada, além da perda desta, responderá o contrato pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos, ou ainda, se for o caso, cobrada judicialmente.

ANEXO VIII
MATRIZ DE RISCO

Categoria do Risco	Descrição	Consequência	Medidas Mitigadoras	Alocação do Risco
Risco atinente ao Tempo da Execução	Atraso na execução do objeto contratual por culpa da CONTRATADA .	Aumento do custo do produto e/ou do serviço.	Diligência da CONTRATADA na execução contratual.	CONTRATADA
	Fatos retardadores ou impeditivos da execução do Contrato próprios do risco ordinário da atividade empresarial ou da execução.	Aumento do custo do produto e/ou do serviço.	Planejamento empresarial.	CONTRATADA
	Fatos retardadores ou impeditivos da execução do Contrato que não estejam na sua área ordinária, tais como fatos do princípio, caso fortuito ou de força maior, bem como o retardamento determinado pelo CONTRATANTE , que comprovadamente repercuta no preço da CONTRATADA .	Aumento do custo do produto e/ou do serviço.	Revisão de preço.	CONTRATANTE
Risco da Atividade Empresarial	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro da CONTRATADA na avaliação da hipótese de incidência tributária.	Aumento ou diminuição do lucro do Contratado.	Planejamento tributário.	CONTRATADA
	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a execução do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra.	Aumento do custo do produto e/ou do serviço.	Repactuação anual de preço.	CONTRATANTE
	Elevação dos custos operacionais definidos na linha anterior, quando superior ao apurado conforme Cláusula de Equilíbrio Econômico-Financeiro do Contrato.	Aumento do custo do produto e/ou do serviço.	Planejamento empresarial.	CONTRATADA

	Variação cambial de natureza ordinária (Dólar, Euro ou outra moeda reconhecidamente nacional)	Aumento do custo do produto e/ou do serviço.	Planejamento empresarial.	CONTRATADA
Riscos Trabalhista e Previdenciário	Responsabilização do Banco da Amazônia por verbas trabalhistas e previdenciárias dos profissionais do Contratado alocados na execução do objeto contratual.	Geração de custos trabalhistas e/ou previdenciários para o CONTRATANTE, além de eventuais honorários advocatícios, multas e verbas sucumbenciais.	Ressarcimento, pela CONTRATADA, ou retenção de pagamento e compensação com valores a este devido, da quantia despendida pelo CONTRATANTE.	CONTRATADA
Risco Tributário e Fiscal (Não Tributário).	Responsabilização do CONTRATANTE por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa do CONTRATANTE.	Débito ou crédito tributário ou fiscal (não tributário).	Ressarcimento, pela CONTRATADA, ou retenção de pagamento e compensação com valores a este devido, da quantia despendida pelo CONTRATANTE.	CONTRATADA



ANEXO IX
PROPOSTA COMERCIAL



PROPOSTA EMERGENCIAL | PRORROGAÇÃO CONTRATUAL – REDE CORPORATIVA

Belém, 31 de outubro de 2025.

AO: BANCO DA AMAZÔNIA

ATT: Dayvid Gomes Vital Fares - Coordenador - CORED

Referente ao Contrato nº: 2020/218
Data de Assinatura Original: 15/12/2020

Nesta.

Prezados Senhores,

A CLARO S/A - CLARO, com sede na Rua Henri Dunant, 780, Santo Amaro, São Paulo – SP, inscrita no CNPJ sob o Nº 40.432.544/0001-47, através do seu Escritório Regional em Belém - PA, situado na Trav. Quintino Bocaiúva 1186, CEP: 66.053-240, vem através desta, apresentar a V. Sas., sua proposta emergencial de prorrogação contratual para para o fornecimento e manutenção dos serviços de REDE PRIVADA DE COMUNICAÇÃO MULTISSERVIÇO MPLS, ACESSOS À REDE INTERNET com proteção anti-DDoS, e PRESTAÇÃO DE SERVIÇOS DE REDE DE ALTA VELOCIDADE (LAN-TO-LAN) referente ao Lotes 01, 02 e 03, conforme condições, quantidades e exigências estabelecidas no documento em referência.

LUCIANA COSTA CONCEIÇÃO

Gerente de Contas

CLARO S/A

Diretoria de Vendas Governo

Tel.: + 55 21 91 4005-8254 / Cel.: 91 984258678

Email: luciana.conceicao@claro.com.br



PROPOSTA ORIENTATIVA – REDE CORPORATIVA BANCO DA AMAZÔNIA

A presente proposta tem caráter excepcional e temporário, com prazo de 6 (seis) meses, contados a partir do término da vigência do Contrato nº 2020/218, celebrado em 15/12/2020, preservando-se integralmente as condições técnicas, comerciais e de atendimento atualmente praticadas.

PROPOSTA DE PREÇOS

LOTE	Descrição	Valor Mensal	Valor Semestral
		(R\$)	(R\$)
LOTE 01	REDE PRIVADA DE COMUNICAÇÃO MULTISSERVIÇO MPLS COM ENLACES DE TRANSMISSÃO, HARDWARE, SOFTWARE PARA A INTERLIGAÇÃO CORPORATIVA DAS REDES LOCAIS (LAN) E METROPOLITANAS (MAN), ABRANGENDO A DIREÇÃO GERAL, SUPERINTENDÊNCIAS, AGÊNCIAS, POSTOS BANCÁRIOS e REDE PARCEIROS, COM BALANCEAMENTO SEGURO DE CIRCUITOS, FORNECIMENTO DE SOLUÇÃO WIFI, INCLUINDO SISTEMA DE GERENCIAMENTO E MONITORAÇÃO WAN.	R\$ 559.020,33	R\$ 3.354.122,01
LOTE 02	PRESTAÇÃO DE SERVIÇOS DE REDE DE ALTA VELOCIDADE (LAN-TO-LAN). ATRAVÉS DE CIRCUITOS DE ALTA VELOCIDADE PARA CONTINGÊNCIA E REPLICAÇÃO DO BANCO DE DADOS ENTRE OS DATACENTERS PRIMÁRIO E SECUNDÁRIO DA CONTRATANTE, UTILIZANDO ACESSOS DE FIBRA ÓPTICA EM ANEL E INTERFACES GIGA ETHERNET (GE) A SEREM PRONTAMENTE UTILIZADOS EM CASO DE DESASTRE/FALHAS NO SITE PRINCIPAL.	R\$ 92.542,87	R\$ 555.257,19
LOTE 03	ACESSOS A REDE INTERNET NOS DATACENTERS DA CONTRATANTE COM FORNECIMENTO DE SERVIÇO DE PROTEÇÃO ANTI-DDOS VOLUMÉTRICO, ANTI-DDOS CAMADA DE APLICAÇÃO, SEGURANÇA E PROTEÇÃO DA REDE LAN (NGFW). (OPERADORA 01).	R\$ 101.628,71	R\$ 609.772,28
VALOR TOTAL GERAL		R\$ 753.191,91	R\$ 4.519.151,48

VALOR MENSAL: R\$ 753.191,91 (por extenso: Setecentos e cinquenta e três mil cento e noventa e um reais e noventa e um centavos)

VALOR SEMESTRAL: R\$ 4.519.151,48 (por extenso: Quatro milhões quinhentos e dezenove mil cento e cinquenta e um reais e quarenta e oito centavos)



PROPOSTA ORIENTATIVA – REDE CORPORATIVA BANCO DA AMAZÔNIA

A CLARO S/, declara que nos preços propostos estão incluídos todos os custos e despesas, inclusive mão de obra, taxas, impostos, tributos, contribuições sociais, para-fiscais, comerciais, serviços de entrega e outros inerentes ao objeto do Termos de Referência,

Prazo de validade: 60 (sessenta) dias úteis, após sua apresentação.

1. DADOS DA EMPRESA E DO SEU REPRESENTANTE LEGAL

1.1. Dados da empresa:

- a) Razão Social: **CLARO S/A – CLARO**
- b) CNPJ/MF: 40.432.544/0001-47
- c) Endereço Sede: RUA HENRI DUNANT, 780, SANTO AMARO
- d) Cidade/UF: SÃO PAULO/SP – BRASIL
- e) CEP: 04.709-110
- f) Tel./Fax: 55 21 91 4005-8254
- g) E-mail: luciana.conceicao@claro.com.br
- h) Banco/Agência: Banco do Brasil S/A / 3070-8
- i) Conta Corrente: 6014-3

1.2. Dados do representante legal da empresa para assinatura do contrato:

- j) Nome: Luciana Costa Conceição
- k) Endereço: Tv. Quintino Bocaiúva, 1186 - Reduto
- l) CEP: 66053-240
- m) Cidade/UF: Belém/PA
- n) CPF/MF: 802.396.502-63
- o) RG/Órgão Expedidor: 14580 – CREA/PA
- p) Telefone/E-mail: luciana.conceicao@claro.com.br

2. CONDIÇÕES DA PRORROGAÇÃO

Prazo: extensão emergencial de 6 (seis) meses, a partir de 15/12/2025.

Escopo: integralmente mantido conforme objeto do contrato vigente.

Valores e Condições Comerciais: permanecem inalterados, em conformidade com o contrato atual.

Garantias Operacionais: preservação dos SLAs, suporte técnico e níveis de serviço contratados.



PROPOSTA ORIENTATIVA – REDE CORPORATIVA BANCO DA AMAZÔNIA

3. VALIDADE DA PROPOSTA

Esta proposta tem validade até 60 (sessenta) dias, devendo ser formalizada mediante assinatura de Termo Aditivo.

4. CONCLUSÃO

Na certeza de estarmos oferecendo a melhor solução às necessidades de prestação de serviço de Telecomunicações por meio de uma Rede Privativa de Comunicação para o **BANCO DA AMAZÔNIA S.A.**, voltamos a nos colocar à disposição, através desta Diretoria Regional de Vendas Corporativas, pelos telefones 55 21 (91) 4005-8254 e 984258678.

Declaramos, ainda, estarmos de acordo com todas as demais condições constantes do Termo de Referência do BANCO DA AMAZÔNIA S.A. e seus Anexos e a elas nos submetemos.

Sendo o que se apresenta para o momento, subscrevemo-nos.

Belém, 31 de outubro de 2025

LUCIANA COSTA CONCEIÇÃO

Gerente de Contas

CLARO S/A

Diretoria de Vendas Governo

Tel.: + 55 21 91 4005-8254 / Cel.: 91 984258678

Email: luciana.conceicao@claro.com.br

Certificado de Conclusão

Identificação de envelope: 3200B26D-EF67-4C64-8DE3-B02070BDC28C

Status: Concluído

Assunto: BASA/Docusign: CLARO S.A. - CONTRATO 2025-227.pdf

Envelope fonte:

Documentar páginas: 73

Assinaturas: 6

Certificar páginas: 5

Rubrica: 0

Assinatura guiada: Ativado

Selo com Envelopeld (ID do envelope): Ativado

Fuso horário: (UTC-03:00) Brasília

Remetente do envelope:

assinatura.contratos@basa.com.br

Rua Santo Antonio, N.17 - Sala F - Centro

Eusebio, CE 61760000

assinatura.contratos@basa.com.br

Endereço IP: 163.116.233.60

Rastreamento de registros

Status: Original

Portador: assinatura.contratos@basa.com.br

Local: DocuSign

12/12/2025 16:51:49

assinatura.contratos@basa.com.br

Eventos do signatário

Bruna Eline da Silva Cavalcante

bruna.cavalcante@basa.com.br

Nível de segurança: E-mail, Autenticação da conta
(Nenhuma)**Assinatura**

Assinado por:



FB53D5B7727F4A...

Registro de hora e data

Enviado: 12/12/2025 16:54:29

Visualizado: 12/12/2025 17:13:42

Assinado: 12/12/2025 17:14:17

Adoção de assinatura: Estilo pré-selecionado

Usando endereço IP: 163.116.230.153

Termos de Assinatura e Registro Eletrônico:

Não oferecido através da Docusign

Luciana Costa Conceição

luciana.conceicao@claro.com.br

Nível de segurança: E-mail, Autenticação da conta
(Nenhuma)

Assinado por:



1A49D0B4F0BA4DF...

Enviado: 12/12/2025 16:54:29

Visualizado: 12/12/2025 16:57:13

Assinado: 12/12/2025 17:04:47

Adoção de assinatura: Estilo pré-selecionado

Usando endereço IP: 24.239.164.83

Termos de Assinatura e Registro Eletrônico:

Aceito: 12/12/2025 16:57:13

ID: 44330ecc-28e3-49fa-a65c-fdbcdc1b5fea

Eventos do signatário presencial**Assinatura****Registro de hora e data****Eventos de entrega do editor****Status****Registro de hora e data****Evento de entrega do agente****Status****Registro de hora e data****Eventos de entrega intermediários****Status****Registro de hora e data****Eventos de entrega certificados****Status****Registro de hora e data****Eventos de cópia****Status****Registro de hora e data**

alan barros costa

Copiado

Enviado: 12/12/2025 16:54:29

alan.costa@basa.com.br

Nível de segurança: E-mail, Autenticação da conta
(Nenhuma)**Termos de Assinatura e Registro Eletrônico:**

Aceito: 26/09/2025 10:09:47

ID: 306d2d1d-f37b-43cb-8cff-b7a3f1d65efa

Eventos com testemunhas**Assinatura****Registro de hora e data**

Eventos do tabelião	Assinatura	Registro de hora e data
---------------------	------------	-------------------------

Eventos de resumo do envelope	Status	Carimbo de data/hora
-------------------------------	--------	----------------------

Envelope enviado	Com hash/criptografado	12/12/2025 16:54:29
Entrega certificada	Segurança verificada	12/12/2025 16:57:13
Assinatura concluída	Segurança verificada	12/12/2025 17:04:47
Concluído	Segurança verificada	12/12/2025 17:14:17

Eventos de pagamento	Status	Carimbo de data/hora
----------------------	--------	----------------------

Termos de Assinatura e Registro Eletrônico
--

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, HCITIS ISV OBO BASA BANCO DA AMAZONIA (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact HCITIS ISV OBO BASA BANCO DA AMAZONIA:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: jonatas.nobre@basa.com.br

To advise HCITIS ISV OBO BASA BANCO DA AMAZONIA of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at jonatas.nobre@basa.com.br and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from HCITIS ISV OBO BASA BANCO DA AMAZONIA

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to jonatas.nobre@basa.com.br and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with HCITIS ISV OBO BASA BANCO DA AMAZONIA

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an email to jonatas.nobre@basa.com.br and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: <https://support.docusign.com/guides/signer-guide-signing-system-requirements>.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify HCITIS ISV OBO BASA BANCO DA AMAZONIA as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by HCITIS ISV OBO BASA BANCO DA AMAZONIA during the course of your relationship with HCITIS ISV OBO BASA BANCO DA AMAZONIA.