**TERMO DE REFERÊNCIA**

1. OBJETO
   1. Contratação de 2 (dois) grupos de serviços de “Rede Integrada de Conectividade Empresarial” permanente, dedicados e exclusivos, de operadoras de telecomunicações distintas, baseado em infraestrutura de fibra-óptica, mediante locação de equipamentos, gerenciamento pró ativo, solução anti-DDoS e suporte técnico 24x7, conforme especificações técnicas descritas nesse documento.
2. DETALHAMENTO DO OBJETO
   1. Serão contratados 2 (dois) grupos de serviços de “Rede Integrada de Conectividade Empresarial” de características técnicas idênticas, conforme tabela abaixo:

|  |  |  |  |
| --- | --- | --- | --- |
| Grupo | Descrição | Serviços | Quantidade |
| 1 | Serviços de “Rede Integrada de Conectividade Empresarial” permanente, dedicados e exclusivos, de operadoras de telecomunicações distintas, baseado em infraestrutura de fibra-óptica, mediante **ativação de circuito**, **locação de equipamentos**, **gerenciamento pró-ativo**, **solução anti-DDoS** e **suporte técnico 24x7**, por 60 (sessenta) meses | Acesso IP Internet, com velocidade de 1 Gbps; | 3 |
| Acesso IP Internet, com velocidade de 300 Mbps; | 1 |
| Acesso IP Internet, com velocidade de 100 Mbps; | 1 |
| Acesso IP Internet, com velocidade de 50 Mbps; | 1 |
| Acesso IP Lan-to-Lan, com velocidade de 300 Mbps; | 2 |
| Microsoft Azure ExpressRoute, com velocidade de 200 Mbps; | 1 |
| Google Cloud Partner Interconnect, com velocidade de 200 Mbps; | 1 |
| Interligação Microsoft Azure ExpressRoute e Google Cloud Partner Interconnect, com velocidade de 200 Mbps; | 1 |
| 2 | Serviços de “Rede Integrada de Conectividade Empresarial” permanente, dedicados e exclusivos, de operadoras de telecomunicações distintas, baseado em infraestrutura de fibra-óptica, mediante **ativação de circuito**, **locação de equipamentos**, **gerenciamento pró-ativo**, **solução anti-DDoS** e **suporte técnico 24x7**, por 60 (sessenta) meses | Acesso IP Internet, com velocidade de 1 Gbps; | 3 |
| Acesso IP Internet, com velocidade de 300 Mbps; | 1 |
| Acesso IP Internet, com velocidade de 100 Mbps; | 1 |
| Acesso IP Internet, com velocidade de 50 Mbps; | 1 |
| Acesso IP Lan-to-Lan, com velocidade de 300 Mbps; | 2 |
| Microsoft Azure ExpressRoute, com velocidade de 200 Mbps; | 1 |
| Google Cloud Partner Interconnect, com velocidade de 200 Mbps; | 1 |
| Interligação Microsoft Azure ExpressRoute e Google Cloud Partner Interconnect, com velocidade de 200 Mbps; | 1 |

* 1. Sabendo-se que a intenção dessa contratação é oferecer uma solução de alta disponibilidade contingenciada de acesso à Internet e Comunicação entre as Entidades e Órgãos Nacionais do Sistema Indústria, os itens acima deverão ser adjudicados a **empresas distintas**, que deverão possuir infraestrutura de comunicação de dados diferentes e independentes. Nesse sentido, **as prestadoras de serviço somente poderão ser vencedoras de um único item**.
     1. Todas as participantes poderão apresentar proposta para os 2 (dois) grupos de serviços. Entretanto, em observância ao disposto no item 2.2 supra, a vencedora do “grupo 1” terá sua proposta automaticamente desconsiderada para o “grupo 2” do chamamento público.
  2. Os serviços de “Rede Integrada de Conectividade Empresarial” deverão ser prestados no seguinte endereço:
     1. **Entidades e Órgãos Nacionais do Sistema Indústria** - SBN Quadra 01, Bloco C, Ed. Roberto Simonsen, 11° andar, CPD, CEP 70040-903 – Brasília/DF;
     2. **SESI Lab** - ST SCTS, 01, Bloco A, Zona Cívico-Administrativa, Ed. SESI Lab, Andar Mezanino, CPD, CEP 70070-150 – Brasília/DF;
     3. **ISI Biodiversidade** - Fazenda Barreiros e Fazenda Flavia Maria, Gleba A e B, Ed. ISI Biodiversidade, Alphaville Brasília, CEP 72897-090 – Cidade Ocidental/GO;
     4. **CNI São Paulo** - Rua Surubim, 504, 16º andar, CPD, Brooklin Novo, CEP 04571-050, São Paulo/SP;
     5. **Instituto SESI SENAI de Tecnologias Educacionais** - SBN, Quadra 02, Bloco J, 3º subsolo, CPD, CEP 70040-010 – Brasília/DF;
     6. **Galpão CNI** - SAAN, Quadra 02, Lotes 455/465, CEP 70632-250 - Brasília/DF;
     7. **Residência Oficial CNI** - QI 21, Conj. 06, Casa 28, Lago Sul, CEP 71655-260 – Brasília/DF;
     8. **Cloud Pública Microsoft Azure Cloud**;
     9. **Cloud Pública Google Cloud Plataform**;

1. REQUISITOS TÉCNICOS
   1. Os serviços referentes aos “Grupos 1 e 2” do objeto devem atender por completo às seguintes especificações técnicas mínimas para cada acesso a ser contratado. Quando não explicitamente indicado, todas as condições a seguir são obrigatórias para ambos os itens da seleção.
   2. Especificações Técnicas Comuns:
      1. Os serviços de “Rede Integrada de Conectividade Empresarial” contratados deverão apresentar, no mínimo, as seguintes especificações técnicas:
         1. Deverá fornecer e manter várias conexões de rede em várias localidades;
         2. Cada localidade terá um tipo específico de conexão de rede, fornecida por uma operadora específica;
         3. A CONTRATADA deverá garantir que todas as conexões de rede estejam em pleno funcionamento e atendam a todas as especificações durante toda a vigência do contrato;
         4. Ser provido com base em uma infraestrutura de fibra-óptica, como meio de acesso, vedada a utilização de qualquer outra tecnologia de acesso;
         5. Todos os equipamentos e links devem suportar tanto IPv4 quanto IPv6, sendo que este último deve estar implementado de forma nativa em pilha dupla;
         6. O acesso deverá permitir qualquer tipo de aplicação através da internet, inclusive VoIP, não podendo o contratado impor restrições ao uso de quaisquer protocolos, aplicações, endereços, portas ou URLs;
         7. O(s) equipamento(s) fornecido(s) pelo contratado deverá(ão) ser instalado(s) com a última versão de firmware disponibilizada pelo fabricante, de modo a minimizar a probabilidade de atualização de versões assim que a solução estiver totalmente operacional;
         8. Prover equipamentos e respectivos cabos de comunicação de dados novos e de primeiro uso, independentes para cada um dos acessos contratados, a serem instalados nas dependências das contratadas;
         9. Ser dimensionado para garantir, em termos de disponibilidade e desempenho, os níveis de serviços exigidos no item 5 (Acordo de Nível de Serviços e Multas Aplicáveis);
         10. Ser dedicado aos serviços de acesso à internet e lan-to-lan durante o transcorrer do contrato, podendo somente ser desativado ao término deste ou em caso de substituição, sujeita à autorização das contratantes;
         11. Possuir portas WAN e/ou LAN compatíveis, em tipo e quantidade, com a solução de acesso ao backbone definida pelo contratado;
         12. Suportar protocolo de gerenciamento SNMP (Simple Network Management Protocol), de modo a ser acessível pelos sistemas de gerência de redes das contratantes, incluindo configuração de envio de traps;
         13. Ser gerenciável via SSHv2 (Secure Shell) e console (porta serial RS232C);
         14. Garantir que as portas SSH e Telnet nos roteadores sejam bloqueadas para acesso público, a fim de prevenir acessos não autorizados e potenciais ameaças de segurança;
             1. O acesso a essas portas devem ser estritamente controladas e permitidas apenas para administradores de rede autorizados a partir de endereços IP específicos.
      2. A contratada deve implementar e manter medidas de segurança adequadas para garantir o cumprimento desta cláusula durante toda a vigência do contrato.
   3. **Especificações Técnicas para serviços de “Acesso IP Internet”:**
      1. Todos os serviços deverão possuir um link dedicado para conexão à infraestrutura de comunicação da contratada e a internet por toda a vigência contratual, nas seguintes velocidades:
         1. 1 Gbps;
         2. 300 Mbps;
         3. 100 Mbps;
         4. 50 Mbps;
      2. O backbone internet do contratado deverá estar diretamente conectado a, pelo menos, três outros sistemas autônomos (AS – Autonomous System) nacionais, e a pelo menos, um sistema autônomo internacional;
      3. Prevenção a ataques de negação de serviço (Anti-DDoS). O contratado será responsável por monitorar, detectar e proativamente mitigar ataques volumétricos, garantindo a disponibilidade do link internet durante o ataque DDoS e evitando a degradação ou saturação da banda contratada. A solução deve prover relatórios de eventos detectados e mitigados;
      4. Disponibilizar servidor DNS (Domain Name Resolution) secundário para cada um dos acessos, capazes de resolver direta e reversamente endereços de internet, para registro no DNS primário do domínio das contratadas;
      5. Implementar NAT (Network Address Translation) estático e dinâmico;
      6. Suporte aos mecanismos de:
         1. Protocolos BGP-4, OSPF e VRRP (ou similar);
         2. Listas de controle de acesso;
         3. Roteamento baseado no endereço de origem do pacote (Policy Based Routing);
      7. CONTRATADA deverá disponibilizar blocos de endereços IP para os Serviços de acesso IP de Internet adequados às necessidades operacionais das CONTRATANTES, incluindo os seguintes blocos já em uso, conforme o quadro abaixo:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Serviço | Localidade | Bloco IP | Quantidade IP |
| 1 | Acesso IP Internet, com velocidade de 1 Gbps. | Entidades e Órgãos Nacionais do Sistema Indústria | /26 | 64 |
| Qualquer Localidade | /29 | 8 |
| 2 | Acesso IP, com velocidade de 300 Mbps | Qualquer Localidade | /29 | 8 |
| 3 | Acesso IP Internet, com velocidade de 100 Mbps. | * + 1. Qualquer Localidade | /30 | 4 |
| 4 | Acesso IP Internet, com velocidade de 50 Mbps; | Qualquer Localidade | /29 | 8 |

* + 1. A CONTRATADA se compromete a avaliar e disponibilizar novos blocos de endereços IP, sempre que necessário para expansão dos serviços, novos links ou incremento de velocidades, em acordo com os procedimentos estabelecidos pelo Registro Regional de Internet relevante e em conformidade com as políticas da Internet Assigned Numbers Authority (IANA), respeitando todas as leis e regulamentos aplicáveis.
    2. A CONTRATADA será responsável por todas as tarefas técnicas associadas à alocação e configuração dos endereços IP, incluindo, mas não se limitando a manutenção de registros, a atualização de DNS e a implementação de medidas de segurança apropriadas;
    3. A CONTRATADA deverá garantir que todos os endereços IP fornecidos estejam livres de quaisquer restrições ou conflitos e sejam totalmente funcionais para uso pelas CONTRATANTES.
    4. A CONTRATADA deverá fornecer suporte técnico à CONTRATANTE para a implementação e manutenção dos endereços IP, incluindo a resolução de quaisquer problemas ou dificuldades técnicas que possam surgir.
    5. A CONTRATADA deverá garantir que a alocação e o uso dos endereços IP estejam em conformidade com todas as leis, regulamentos e políticas aplicáveis, incluindo, mas não se limitando a, as políticas da IANA e do Registro Regional de Internet relevante.
       1. **Proteção Contra Ataques Distribuídos de Negação de Serviços**
          1. 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 (Denial of Service) e DDoS (Distributed Denial of Service) de acordo com os requisitos mínimos a seguir:

Serviços deverão ter pró-atividade para solução e prevenção de incidentes e ataques.

Monitorar disponibilidade e performance de todos os links de dados existentes nesse termo de referência durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana utilizando profissionais de forma dedicada.

Os profissionais devem ser capacitados pelo fornecedor da plataforma de mitigação.

* + - * 1. 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.
        2. 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.
        3. A solução deve suportar a mitigação automática de ataques, utilizando múltiplas técnicas como White List, Black List, 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.
        4. A solução deve implementar mecanismos capazes de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo os 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.

* + - * 1. 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 considerado seguro pela CONTRATADA.
        2. A CONTRATADA deve possuir pelo menos um centro de limpeza nacional com capacidade mínima de mitigação de 1Gbps e um centro de limpeza internacional com capacidade mínima de mitigação de 30Gbps.
        3. A CONTRATADA deve mitigar ataques por 3 horas.
        4. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS (Autonomous System) 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. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.
        6. A CONTRATADA deve disponibilizar um 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.
        7. 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.
        8. 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 da contratada e o CPE do contratante.
        9. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro.
        10. 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.
        11. Em nenhum caso será aceito bloqueio de ataques de DoS e DDoS por ACLs em roteadores de bordas da contratada.
        12. A contratada deve iniciar em até 15 (quinze) minutos a mitigação de ataques.
        13. A CONTRATADA deverá disponibilizar uma Solução de Monitoração de acompanhamento contra ataques DoS e DDoS, que contemple:

Quadro Sinóptico para visualização da ocupação de banda do link Internet e níveis de severidade dos ataques.

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 número de identificação que facilite sua consulta.

Informar a data de início e fim do acompanhamento do alerta.

Volume de ataques sumarizados por hora, dia, semana e mês.

Relatório por tipos de ataques.

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.

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

* 1. **Especificações Técnicas para serviços de “Acesso IP Lan-to-Lan”:**
     1. Os serviços deverão possuir um link dedicado de 300 Mbps para conexão à infraestrutura de comunicação das CONTRADADAS por toda a vigência contratual:

|  |  |  |
| --- | --- | --- |
| Serviço | Localidades | Quantidade |
| Acesso IP Lan-to-Lan, com velocidade de 300 Mbps. | Entidades e Órgãos Nacionais do Sistema Indústria x SESI Lab | 1 |
| Entidades e Órgãos Nacionais do Sistema Indústria x ISI Biodiversidade | 1 |

* 1. **Especificações Técnicas para serviços “Microsoft Azure ExpressRoute” e “Google Cloud Partner Interconnect”:**
     1. Os serviços deverão possuir um link dedicado de 200 Mbps para conexão à infraestrutura de comunicação das CONTRATADAS por toda a vigência contratual:

|  |  |  |
| --- | --- | --- |
| Serviço | Localidades | Quantidade |
| Microsoft Azure ExpressRoute, com velocidade de 200 Mbps. | Entidades e Órgãos Nacionais do Sistema Indústria x Microsoft Azure | 1 |
| Google Cloud Partner Interconnect, com velocidade de 200 Mbps. | Entidades e Órgãos Nacionais do Sistema Indústria x Google Cloud Partner | 1 |

* 1. **Especificações Técnicas para serviços de “Interligação Microsoft Azure ExpressRoute e Google Cloud”:**
     1. Os serviços deverão possuir um link dedicado de 200 Mbps para conexão à infraestrutura de comunicação das clouds, por toda a vigência contratual:

|  |  |  |
| --- | --- | --- |
| Serviço | Localidades | Quantidade |
| Interligação Microsoft Azure ExpressRoute e Google Cloud, com velocidade de 200 Mbps. | Microsoft Azure Cloud x Google Cloud Plataform | 1 |

1. REQUISITOS OPERACIONAIS
   1. **Instalação:**
      1. A CONTRATADA terá o prazo máximo de 60 (sessenta) dias, a contar da assinatura do contrato, para disponibilizar o objeto dessa contratação para pleno uso das CONTRATANTES;
      2. Salienta-se que os 30 (trinta) dias definidos no item acima, serão para instalação da infraestrutura necessária para a viabilização dos serviços contratados.
      3. Devem estar inclusos todos os custos decorrentes dos tributos e encargos trabalhistas, previdenciários, comerciais, além de seguros, fretes, deslocamentos de pessoal e de bens, se houverem, e quaisquer outros custos que incidam direta ou indiretamente na execução do objeto.
      4. Os trabalhos de instalação de qualquer natureza, quando realizados nas dependências das CONTRATANTES, poderão ocorrer em qualquer horário, inclusive fora do período normal de expediente (das 8h às 19h), desde que haja prévio alinhamento e concordância com a CONTRATADA.
         1. O objetivo desta flexibilidade é garantir que o impacto seja o mínimo possível ao ambiente computacional e aos funcionários das CONTRATANTES. A CONTRATADA deverá se esforçar para minimizar quaisquer interrupções ou inconveniências causadas pelas atividades de instalação.
      5. A CONTRATADA deverá comunicar antecipadamente à CONTRATANTE sobre qualquer trabalho de instalação planejado, incluindo a natureza do trabalho, a data e o horário propostos, e quaisquer requisitos ou preparações necessárias.
      6. O aceite definitivo da solução e consequente início do período de prestação dos serviços, se dará após verificação de conformidade e aderência às especificações técnicas exigidas, bem como atendimento dos níveis de serviços contratados e de processo de abertura de chamados, pela equipe técnica das CONTRATANTES, em até cinco dias corridos.
      7. Após o aceite definitivo da solução se iniciará o período de prestação dos serviços para fins de faturamento e de verificação dos serviços.
   2. **Atendimento Comercial:**
      1. CONTRATADA deverá designar um Consultor ou Gerente de Contas para acompanhar o Contrato e indicar o(s) funcionário(s) que estarão designados para atender as solicitações das CONTRATANTES.
      2. A qualquer tempo, as CONTRATANTES poderão solicitar a substituição do referido Consultor ou Gerente de Contas da CONTRATADA desde que entenda que seja benéfico ao desenvolvimento dos serviços.
   3. **Atendimento Técnico:**
      1. A CONTRATADA deverá realizar o atendimento das solicitações de reparo, por meio de número telefônico gratuito (0800) com funcionamento 24 horas por dia e 7 dias por semana, nos prazos definidos no acordo de nível de serviços.
      2. Para cada chamado técnico, a CONTRATADA deverá disponibilizar número de protocolo único para que as CONTRATANTES possam acompanhar a resolução de cada problema, bem como monitorar se os tempos de atendimento técnico estão em conformidade com o Acordo de Nível de Serviços (ANS) estabelecido nesse documento.
      3. Mesmo que não haja paralisação do serviço, a CONTRATADA deverá registrar em seu sistema e notificar aos CONTRATANTES, por e-mail ou outro sistema eletrônico, qualquer falha detectada nos equipamentos sob sua responsabilidade ou nos circuitos.
      4. A CONTRATADA deverá realizar, sempre que necessário, assistência técnica on-site, para solução de problemas de funcionamento, disponibilidade e instabilidade do serviço contratado.
      5. Deverá ser disponibilizado acesso Web para consulta da utilização do serviço contratado, por meio de ferramentas de mercado.
      6. Os serviços de suporte técnico deverão incluir serviços de atualização do(s) equipamento(s) componente(s) da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de software de equipamentos, quando aplicável.
   4. **Gerencia Pró Ativa:**
      1. A CONTRATADA deve implementar um sistema de monitoramento constante que identifique e alerte, em tempo real, qualquer condição anormal e potencialmente prejudicial na infraestrutura ou nos serviços monitorados.
      2. A CONTRATADA será responsável por gerenciar os incidentes detectados, buscando resolver falhas preventivamente e minimizar a ocorrência de interrupções de serviço.
      3. A CONTRATADA fornecerá relatórios regulares sobre disponibilidade, falhas, performance e outros indicadores-chave de desempenho (KPIs) dos serviços monitorados.
      4. A CONTRATADA será encarregada da manutenção regular e preventiva dos equipamentos e softwares, incluindo a atualização de patches de segurança, correção de softwares e otimização contínua do sistema.
      5. A CONTRATADA disponibilizará uma equipe de suporte técnico qualificado 24x7 para responder prontamente a quaisquer incidentes ou questões técnicas levantadas pelas CONTRATANTES.
      6. A CONTRATADA concederá às CONTRATANTES acesso a portal para monitoramento e acompanhamento do desempenho dos serviços, incluindo a abertura e consulta de tickets de suporte (Trouble Ticket).
      7. A CONTRATADA realizará testes de penetração e outras auditorias necessárias para assegurar a integridade e a segurança do ambiente de TI das CONTRATANTES.
      8. A CONTRATADA se compromete a notificar as CONTRATANTES sobre quaisquer alterações significativas, planejadas ou de emergência, que afetem os serviços prestados.
      9. Estas cláusulas buscam garantir que o serviço de gerência pró ativa seja eficiente, transparente e confiável, assegurando o máximo de disponibilidade e performance dos serviços de TI das CONTRATANTES.
   5. **Locação Roteador:**
      1. Todos os roteadores fornecidos pela CONTRATADA devem ser novos, de primeiro uso e especificados para atender ou exceder as necessidades de desempenho e disponibilidade exigidas.
      2. A CONTRATADA deverá oferecer suporte técnico e manutenção contínua para todos os roteadores locados, incluindo a substituição rápida de equipamentos em caso de falha.
      3. Os roteadores locados precisam ser compatíveis com as tecnologias e infraestrutura de TI das CONTRATANTES, assegurando uma integração sem interrupções.
         1. Os roteadores devem suportar os padrões de rede utilizados pelas CONTRATANTES, incluindo, mas não limitados a, Ethernet (IEEE 802.3) e tecnologias de fibra ótica para as conexões WAN.
         2. Devem ser capazes de operar com os protocolos de comunicação em uso, como TCP/IP, UDP, ICMP, e qualquer outro protocolo necessário para manter a conectividade nas redes internas e externas das CONTRATANTES.
         3. Os roteadores precisam ser gerenciáveis e configuráveis através de ferramentas e plataformas de gerenciamento de rede já estabelecidas nas CONTRATANTES, como sistemas baseados no protocolo SNMP (Simple Network Management Protocol).
         4. É necessário que os roteadores possuam interfaces físicas (portas RJ-45, SFP, etc.) e lógicas (VLANs, QoS, etc.) que atendam às especificações técnicas das redes das CONTRATANTES, possibilitando a correta conexão e configuração sem a necessidade de adaptadores ou equipamentos adicionais.
         5. Os roteadores devem atender ou exceder os requisitos mínimos de desempenho (largura de banda, taxa de transferência, capacidade de processamento) necessários para suportar a carga de tráfego gerada pelas atividades das CONTRATANTES.
         6. É imprescindível que os roteadores suportem ambos IPv4 e IPv6, para assegurar a compatibilidade com as infraestruturas de rede existentes e com as futuras expansões que as CONTRATANTES podem realizar.
         7. Os roteadores devem aceitar atualizações de firmware para garantir que novas funcionalidades e correções de segurança possam ser aplicadas, além de manter a compatibilidade com evoluções nas tecnologias de TI.
      4. No fim do contrato, a CONTRATADA será responsável pela desinstalação e retirada dos roteadores, sem custos adicionais para as CONTRATANTES.
2. ACORDO DE NÍVEL DE SERVIÇOS e MULTAS APLICÁVEIS
   1. Para a verificação da qualidade da prestação dos serviços contratados, os seguintes prazos de atendimento deverão ser obedecidos:
      1. Disponibilização dos serviços objeto dessa contratação:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Disponibilização dos serviços | 60 dias | Diário | 3% sobre o Valor Mensal do Serviço, cumulativa enquanto perdurar o descumprimento |

* + 1. Resposta das contestações de Fatura de Serviço encaminhada pela CONTRATANTE, contados a partir da formalização da contestação:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Resposta das contestações de Fiscais/Fatura | 5 dias úteis | Diário | 0,3% sobre o Valor Mensal do Serviço, cumulativa enquanto perdurar o descumprimento |

* + 1. Restabelecimento dos serviços bloqueados indevidamente por motivos administrativos, contados a partir da abertura do chamado:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Restabelecimento dos serviços bloqueados indevidamente | 15 minutos corridos | Diário | 2,5% sobre o Valor Mensal do Serviço, a cada período adicional de 15 minutos de interrupção indevida, cumulativa enquanto perdurar o descumprimento |

* + 1. Disponibilidade mínima dos serviços de acesso:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Disponibilidade | 99,17% a 98,89 | Mensal | 5% sobre o Valor Mensal do Serviço |
| Disponibilidade | 98,89% a 98,61% | Mensal | 10% sobre o Valor Mensal do Serviço |
| Disponibilidade | 98,61% a 98,33% | Mensal | 20% sobre o Valor Mensal do Serviço |
| Disponibilidade | <98,33% | Mensal | 20% sobre o Valor Mensal do Serviço + 5% sobre o Valor Mensal do Serviço a cada 120 minutos |

* + - 1. Resolução do contrato, caso o valor desse indicador tenha sido inferior a 98,33% durante 3 (três) meses consecutivos ou durante 6 (seis) meses quaisquer, mesmo que não consecutivos;
    1. Monitoramento de disponibilidade e performance dos serviços de acesso durante 24 (vinte e quatro) horas, 7 (sete) dias da semana:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Monitoramento | 99,5% a 99,1 | Mensal | 5% sobre o Valor Mensal do Serviço |
| Monitoramento | 99,0% a 98,6% | Mensal | 10% sobre o Valor Mensal do Serviço |
| Monitoramento | 98,5% a 98,1% | Mensal | 20% sobre o Valor Mensal do Serviço |
| Monitoramento | <98,0% | Mensal | 20% sobre o Valor Mensal do Serviço + 5% sobre o Valor Mensal do Serviço a cada 120 minutos |

* + 1. Funcionalidades de monitoramento, detecção e mitigação de ataques em operação durante 24 (vinte e quatro) horas, 7 (sete) dias da semana:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Funcionalidades de Monitoramento, Detecção e Mitigação de Ataques | 24 horas x 7 dias | Mensal | 0,3% sobre o Valor Mensal do Serviço, cumulativa enquanto perdurar o descumprimento |

* + 1. Mitigar ataques de DoS e DDoS:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Mitigação | 3 horas | Mensal | 2,5% sobre o Valor Mensal do Serviço, a cada período adicional de 15 minutos de interrupção indevida, cumulativa enquanto perdurar o descumprimento |

* + 1. Desvios incrementais para perdas de pacote, latência ou velocidade devem seguir a tabela abaixo de descontos nas localidades degradadas:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Perda de Pacotes | 0% a 30% | Mensal | 3% sobre o Valor Mensal do Serviço |
| Perda de Pacotes | +30% a 50% | Mensal | 5% sobre o Valor Mensal do Serviço |
| Perda de Pacotes | +50% | Mensal | 7% sobre o Valor Mensal do Serviço |
| Latência (milissegundos) | +50ms | Mensal | 3% sobre o Valor Mensal do Serviço |
| Velocidade Nominal | <95% | Mensal | 3% sobre o Valor Mensal do Serviço |
| Velocidade Nominal | 95% a 97,5% | Mensal | 5% sobre o Valor Mensal do Serviço |
| Velocidade Nominal | 97,5% a 100% | Mensal | 7% sobre o Valor Mensal do Serviço |

* + 1. Para casos de indisponibilidades dos serviços que compõem a solução disponibilizada ao CONTRATANTE, o tempo máximo de reestabelecimento dos serviços:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Reestabelecimento dos Serviços | Até 6 horas | Mensal | 5% sobre o Valor Mensal do Serviço |
| Reestabelecimento dos Serviços | Até 8 horas | Mensal | 10% sobre o Valor Mensal do Serviço |
| Reestabelecimento dos Serviços | Até 10 horas | Mensal | 20% sobre o Valor Mensal do Serviço |
| Reestabelecimento dos Serviços | Até 12 horas | Mensal | 20% sobre o Valor Mensal do Serviço + 5% sobre o Valor Mensal do Serviço a cada 120 minutos |

* + 1. As informações relativas aos chamados deverão ser atualizadas pela equipe técnica, contadas a partir da abertura do chamado:

|  |  |  |  |
| --- | --- | --- | --- |
| Indicador | SLA | Período | Multa |
| Chamados de Indisponibilidade | Até 2 horas | Mensal | 3% sobre o Valor Mensal do Serviço |

* 1. Nas hipóteses de inexecução das obrigações, não compreendidas nas infrações previstas acima, ao contratado poderá ser aplicada multa diária de 3% (três por cento) sobre o Valor Mensal do Serviço enquanto perdurar o descumprimento;
  2. O serviço será considerado DISPONÍVEL (disponibilidade básica) quando permitir, cumulativamente:
     1. Acesso de estações da Rede Interna das CONTRATANTES a hosts da INTERNET;
     2. Acesso de estações da Rede Interna das CONTRATANTES a outra ponta das CONTRATANTES (no caso de Lan to Lan);
     3. Acesso, a partir da INTERNET, a hosts da Rede Interna e da DMZ;
  3. A disponibilidade mínima dos serviços, será apurada mensalmente, do 1º ao último dia do mês, considerando-se o horário das 0:00 às 24:00, de 2a feira a domingo, através da seguinte fórmula:

Disp = [Tempo de Serviço Disponível]

[Tempo Total]

**onde:**

Disp =Disponibilidade mínima mensal;

[Tempo de Serviço Disponível] = (43.200 – [total de minutos no mês em que o serviço NÃO esteve DISPONÍVEL]);

[Tempo Total] = 43.200 minutos

* 1. As falhas e paralisações que não sejam imputáveis ao CONTRATADO serão expurgadas, assim como os tempos de paralisação em que o CONTRATADO não puder atuar por motivo atribuível aos CONTRATANTES;

1. DO PAGAMENTO
   1. Os valores poderão ser reajustados após 60 meses, caso a vigência venha a ser prorrogada.
   2. O pagamento somente será devido após a conclusão da implantação dos serviços e a emissão do termo de aceitação pelos CONTRATANTES.
   3. O pagamento total será feito no 22º dia do mês subsequente ao da emissão do termo de aceitação pelos CONTRATANTES.
   4. A CONTRATADA deverá emitir uma única fatura mensal consolidada para cada grupo de serviços de “Rede Integrada de Conectividade Empresarial”, englobando todos os links e serviços contratados no âmbito de cada grupo, de modo a simplificar o processo de pagamento e gestão financeira das CONTRATANTES. A fatura deverá detalhar todos os custos individualmente por serviço e localidade, garantindo a clareza e a precisão das informações financeiras prestadas.
   5. Os pagamentos das faturas emitidas pela CONTRATADA estarão condicionados à disponibilização de acesso contínuo a portal, que permita às CONTRATANTES o monitoramento e acompanhamento do desempenho dos serviços contratados. O portal deve proporcionar funcionalidades que incluam, mas não se limitem a abertura e consulta de tickets de suporte (Trouble Ticket), relatórios de desempenho, e atualizações em tempo real referentes a indisponibilidades, performance e quaisquer outros indicadores-chave de desempenho (KPIs). A ausência ou o funcionamento inadequado do portal, que impeça seu uso para o propósito designado, poderá resultar em atrasos no processamento dos pagamentos até que tal funcionalidade seja restabelecida.
2. DA QUALIFICAÇÃO TÉCNICA DA EMPRESA
   1. Por se tratar de um serviço de conectividade com a nuvem pública da Microsoft e Google, a empresa deve comprovar, ser empresa autorizada a comercializar os serviços de ambos os provedores de serviços de nuvem pública nomeados e exigidos para esta contratação (Google Cloud Platform e Microsoft Azure).
      1. Essa comprovação deverá ser feita por meio de declaração específica de cada um dos provedores de nuvem mencionados ou por meio de informação disponível ou acessível no site oficial deles.
   2. Comprovação de aptidão para o desempenho de atividade pertinente e compatível com o objeto da seleção, por meio da apresentação de 01 (um) ou mais atestados fornecidos por pessoa jurídica, de direito público ou privado, no qual conste a prestação de serviço e/ou a realização de fornecimento da mesma natureza ou similar ao objeto desta seleção. O atestado deve ser datado e assinado e deverá conter informações que permitam a identificação correta do contratante e do prestador do serviço, tais como:
3. Nome, CNPJ e endereço do emitente da certidão;
4. Nome, CNPJ e endereço da empresa que prestou o serviço ao emitente; e
5. Identificação do signatário (nome, cargo ou função que exerce junto à emitente).
6. DAS OBRIGAÇÕES DA EMPRESA CONTRATADA
   1. Cumprir o objeto contratado nos termos e condições constantes do Contrato, do Chamamento e seus anexos, bem como da respectiva proposta de preços da CONTRATADA, cabendo-lhe ainda a coordenação dos serviços, responsabilizando-se, legal, administrativa e tecnicamente pelos mesmos.
   2. Cumprir os prazos e o cronograma de execução e/ou entrega dos serviços e/ou materiais e equipamentos definidos no contrato.
   3. Cientificar, imediatamente e por escrito, os CONTRATANTES, qualquer anormalidade que verificar durante a execução dos serviços e/ou fornecimentos.
   4. Prestar esclarecimentos, imediatamente e por escrito, aos CONTRATANTES, sempre que por estes solicitado.
   5. Se comprometer a manter ininterruptos todos os links e serviços de "Rede Integrada de Conectividade Empresarial" previstos no contrato, independentemente de eventuais equívocos ou erros na emissão das faturas dos serviços prestados. Em nenhuma hipótese, falhas administrativas relacionadas à faturamento justificarão a interrupção, bloqueio ou suspensão dos serviços contratados pelos CONTRATANTES. Qualquer descontinuidade dos serviços por motivos administrativos está sujeita às penalidades previstas no Acordo de Nível de Serviços (ANS), assegurando assim a continuidade dos negócios e operações das CONTRATANTES.
7. OBRIGAÇÕES DA CONTRATANTE
   1. Efetuar os pagamentos devidos à CONTRATADA de acordo com o estabelecido neste Termo de Referência.
   2. Fornecer e colocar à disposição da CONTRATADA todos os elementos e informações que se fizerem necessários à execução dos serviços e/ou fornecimentos.
   3. Informar a CONTRATADA, por escrito, as razões que motivaram eventual rejeição dos serviços e/ou fornecimentos contratados.
   4. Notificar, formal e tempestivamente a CONTRATADA sobre as irregularidades observadas no cumprimento do contrato.
8. Segurança da informação
   1. Visando a SEGURANÇA DA INFORMAÇÃO, caberá às PARTES:
      1. Cada PARTE será única responsável pela seleção, implementação, e manutenção de procedimentos e políticas de segurança que sejam suficientes para garantir que: (i) o uso da conexão de rede por tal parte (e o uso do patrimônio de informações da CONTRATANTE, pela CONTRATADA) seja seguro e utilizado somente para fins autorizados, e (ii) os registros e dados de negócios de tal parte estejam protegidos contra acesso ou uso indevidos, alteração, perda ou destruição.
      2. Qualquer terceira parte que conecte um dispositivo a uma rede da CONTRATANTE deverá ser autorizada pelo Encarregado de Segurança de TI local. O Fornecedor deverá prover proteção contra o uso externo não autorizado, modificação, divulgação ou destruição, acidental ou intencional, do patrimônio da CONTRATANTE. A terceira parte será responsável pela segurança do dispositivo, através de antivírus e patches, para proteger o patrimônio de informações da CONTRATANTE. Qualquer dispositivo pertencente a uma terceira parte, e que armazene ativos de informações da CONTRATANTE, deverá ser criptografado.
         1. Somente usuários autorizados pela CONTRATANTE poderão acessar as informações e dados contidos na infraestrutura da CONTRATANTE ou na infraestrutura de terceiros contratados ou utilizados pela CONTRATANTE. A CONTRATANTE deverá deter o poder de decisão final, a respeito de quem estará autorizado a acessar os dados e informações, incluindo o próprio pessoal da CONTRATANTE, o pessoal da CONTRATADA, todo o pessoal subcontratado, e qualquer outra terceira parte. Todos os acessos deverão atender às Normas e políticas de tecnologia da informação da CONTRATANTE.
         2. Serão concedidas somente autorizações de acessos individuais (login e senha). Contas genéricas ou compartilhadas são absolutamente proibidas.
         3. Dados ou informações sobre a CONTRATANTE, ou contidos na infraestrutura da CONTRATANTE, quer possuídos, ou cedidos, ou hospedados nas instalações de uma terceira parte, ou na infraestrutura de um Fornecedor de Serviços de Aplicativos, não deverão ser divulgadas a quaisquer terceiras partes, sem a prévia aprovação por escrito da CONTRATANTE.
   2. Visando a SEGURANÇA DA INFORMAÇÃO, caberá a CONTRATADA:
      1. Obedecer às normas, procedimentos e Políticas de Tecnologia da Informação da CONTRATANTE, com todos os regulamentos e todas as atualizações correspondentes deste enquadramento, relativas aos países a partir dos quais a CONTRATADA preste os serviços ou hospede aplicativos ou dados.
      2. Preservar a disponibilidade e precisão das informações dos processos suportados e proteger as informações confidenciais e proprietárias, bem como os direitos de propriedade intelectual da CONTRATANTE.
      3. Assegurar que o acordo de confidencialidade e as obrigações deste CONTRATO sejam atendidos por seus diretores, funcionários, representantes, agentes, e quaisquer outros subcontratados que irão executar tarefas descritas neste CONTRATO, antes da CONTRATADA direcioná-los à prestação dos serviços objeto deste CONTRATO.
         1. As alterações relativas aos aplicativos, arquitetura, procedimentos operacionais, procedimentos de segurança e sua respectiva avaliação de riscos, deverão ser comunicadas antecipadamente.
      4. Oferecer a sua máxima cooperação, para permitir que a CONTRATANTE realize a verificação de conformidade dos produtos fornecidos e/ou serviços prestados.
      5. Atender aos requisitos de governança de tecnologia da informação da CONTRATANTE, o que implica em fornecer informações úteis sobre: (i) infraestrutura / arquitetura de tecnologia da informação e de segurança atualizadas, (ii) organização de tecnologia da informação responsável pelo serviço; e (iii) alterações relativas à arquitetura e procedimentos de segurança, e sua correspondente avaliação de riscos.
      6. Responsabilizar-se exclusivamente perante o CONTRATANTE sobre todas as considerações de segurança de TI. Sob nenhuma circunstância, a CONTRATANTE assumirá ou aceitará o compartilhamento de responsabilidade entre o Fornecedor e qualquer outra terceira parte, incluindo parceiros de negócios e subcontratados do Fornecedor.
      7. Assegurar que todas as atividades do serviço mantenham adequadamente os registros de negócios apropriados, de acordo com as melhores práticas da indústria e em conformidade com as leis e regulamentações aplicáveis, e assegurar também que os documentos estejam protegidos contra acesso ou uso indevidos, perda, alteração ou destruição. A CONTRATADA deverá realizar revisões regulares para detectar potenciais problemas de segurança. A CONTRATADA poderá ser obrigada a revelar as configurações, o processo de revisão, e os resultados.
      8. Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando a CONTRATANTE de qualquer responsabilidade.
      9. Responsabilizar-se única e exclusivamente por todas as medidas de segurança para garantir a proteção de seus sistemas e redes internas, isentando a CONTRATANTE de qualquer responsabilidade.
      10. Juntamente com a definição de requisitos de negócios para novos sistemas ou serviços de informação, ou melhorias em sistemas ou serviços de informação existentes, a CONTRATADA deverá assegurar que a avaliação de segurança seja realizada e que controles de segurança apropriado sejam identificados e incorporados aos requisitos. A avaliação e os controles de segurança a serem incluídos deverão ser analisados e aprovados pela CONTRATANTE.
      11. Não deverá estabelecer qualquer tipo de link de comunicação de dados entre as suas redes e sistemas e os da CONTRATANTE, incluindo, mas não se limitando a atividades de supervisão, intervenção remota, e qualquer tipo de transferência de dados, por qualquer meio, incluindo, mas não se limitando a links diretos permanentes, Internet, VPN [rede privada virtual], ou dial-up [acesso por linha discada], sem a aprovação da CONTRATANTE.
      12. Garantir que o ambiente de Tecnologia da Informação, em seu lado, assegure a integridade, disponibilidade e confidencialidade do patrimônio de Tecnologia da Informação da CONTRATANTE, incluindo dados, informações e direitos de propriedade intelectual.
          1. Somente usuários autenticados e autorizados, com uma data de expiração de usuário pré-definida, deverão ter permissão para acessar sistemas da CONTRATANTE e o prazo de acesso deverá ser restrito.
          2. Deverão ser mantidos logs de auditoria completos, nos níveis de conexão, sistema operacional, e aplicativos. A CONTRATANTE se reserva o direito de supervisionar em tempo real, gravar e utilizar os dados armazenados das conexões.
          3. Todas as conexões com a CONTRATADA deverão ser criptografadas e serão estabelecidas somente através de firewalls da CONTRATANTE. Somente serão permitidos hosts e protocolos previamente autorizados.
      13. Notificar imediatamente a CONTRATANTE, sempre que qualquer funcionário autorizado da CONTRATADA deixe a empresa, ou já não necessite de acesso, ou tenham sido modificadas as responsabilidades para acessar qualquer patrimônio de informações da CONTRATANTE.
          1. Assim que termine a prestação do serviço pela CONTRATADA, por qualquer razão, normal ou anormal, todos os acessos deverão ser imediatamente revogados. A CONTRATADA não será mais autorizada a acessar o patrimônio de informações da CONTRATANTE.
          2. Todas as informações de propriedade da CONTRATANTE deverão ser enviadas à CONTRATANTE, em duas cópias, sendo em seguida removidas com segurança de todos os dispositivos.
      14. Rever a qualquer tempo o acesso de seus empregados ao patrimônio de informações da CONTRATANTE, e prontamente corrigir qualquer discrepância em potencial. Mediante solicitação da CONTRATANTE, a CONTRATADA deverá revelar os resultados da última análise de acessos, bem como as respectivas ações corretivas.
      15. Não utilizar qualquer criptografia desenvolvida internamente, para proteger as informações, os aplicativos ou a infraestrutura da CONTRATANTE. Quaisquer algoritmos simétricos, assimétricos, ou de hashing, utilizado na infraestrutura da CONTRATANTE, deverá utilizar algoritmos e ferramentas bem conhecidos, publicados, apresentados à comunidade global de criptografia, e adotados como padrão da indústria.
          1. A resistência dos algoritmos de criptografia deverá ser a mais alta possível, aprovada pelo CSO [Chief Security Officer / Chefe de Segurança] local da CONTRATANTE, e em conformidade com os requisitos de negócios da CONTRATANTE e com a legislação aplicável.
          2. Conexões que utilizem a Internet deverão ser protegidas utilizando tecnologias de criptografia, adotados como padrão de mercado.
          3. Deverão ser criptografados todos os dispositivos móveis e portáteis utilizados para prover o serviço à CONTRATANTE e que contenham dados confidenciais.
      16. Prover a CONTRATANTE uma lista com os nomes e funções dos funcionários que terão acesso aos Locais da CONTRATANTE. Pessoas incluídas na lista acima referida deverão apresentar-se na recepção do Local da CONTRATANTE, onde receberão um cartão de visitante ou crachá, que deverão portar de forma visível, durante todo o tempo de permanência nas instalações da CONTRATANTE.
          1. Se, por qualquer motivo, uma pessoa não incluída na lista precise acessar o site, ele ou ela deverá ser registrado na recepção, mediante apresentação de sua identificação com foto, ou passaporte. A referida pessoa deverá ser acompanhada por um colaborador da CONTRATANTE, em todos os momentos.
          2. Caso algum membro do pessoal da CONTRATADA, quer previamente autorizado através da lista ou não, necessite acessar áreas sensíveis (tais como salas de servidores, datacenters, armários de rede, etc.), este deverá ser acompanhado por um colaborador da CONTRATANTE, em todos os momentos.
          3. Se a CONTRATADA necessitar acessar os Locais, fora dos horários de trabalho, a CONTRATANTE deverá informar à CONTRATADA as regras específicas a serem respeitadas.
      17. Designar uma pessoa como responsável pela proteção e descarte seguro dos meios de armazenamento. Caso qualquer mídia de armazenamento precise ser descartada, a CONTRATADA deverá desativá-la de maneira segura, de tal forma que os dados não possam ser recuperados a partir da mesma. A mídia deverá ser descartada utilizando uma terceira parte certificada para realizar descarte seguro, ou destruída fisicamente (após os dados haverem sido apagados) tornando-a completamente inoperante. A desativação / destruição de mídia requer a aprovação prévia da CONTRATANTE e a posterior notificação por esta à CONTRATADA.
      18. Independentemente das tarefas contidas diretamente na atividade de serviço de segurança, ou se o serviço incluir atividades de segurança, a CONTRATADA deverá assegurar que todas as atividades do Serviço atendam às Políticas de Segurança da Informação da CONTRATANTE e às normas e diretrizes de segurança e arquitetura, tanto aquelas existentes no momento da assinatura, quanto àquelas que venham a ser lançadas no futuro. As atividades de segurança deverão proporcionar proteção contra o uso não autorizado, modificação, divulgação ou destruição, acidental ou intencional, para o patrimônio de dados corporativos, oferecendo trilhas de auditoria adequada, e em conformidade com as leis aplicáveis.
   3. Visando a SEGURANÇA DA INFORMAÇÃO, caberá ao CONTRATANTE:
      1. Verificar e controlar a qualquer tempo que os produtos fornecidos e/ou serviços prestados pela CONTRATADA estejam em conformidade com o CONTRATO.
      2. Comunicar à CONTRATADA as regras de segurança estabelecidas em conformidade com a legislação aplicável, bem como as regras de acesso.
      3. Autorizar antecipadamente, conforme sua conveniência, o uso de qualquer tipo de mídia de armazenamento, com exceção dos discos rígidos internos e fitas de backup. O uso de mídias de armazenamento removíveis e portáteis, tais como CDs, DVDs, drives USB, Flashdrives, etc., é estritamente proibido.
      4. Autorizar antecipadamente, conforme sua conveniência, todos os ativos de tecnologia da informação da CONTRATANTE que devam deixar as instalações da CONTRATADA (por exemplo, para reparação). Todas as informações armazenadas no dispositivo deverão ser previamente removidas de forma segura. Se a remoção não for prática ou possível, a CONTRATADA será o responsável principal por proteger os ativos contra uso não autorizado, modificação, divulgação, ou destruição, acidental ou intencional.
         1. Previamente à remoção dos ativos das instalações da CONTRATANTE, os controles de segurança a estabelecer deverão ser apresentados pela CONTRATADA e aprovados pela CONTRATANTE.
         2. Se os ativos tiverem de ser desativados ou descartados, as informações deverão ser destruídas de forma segura, e o processo de descarte deverá estar em conformidade com as leis e regulamentos locais.
   4. As auditorias poderão verificar especialmente, mas não limitando, a:
      1. desempenho e qualidade dos serviços prestados;
      2. o cumprimento das obrigações deste CONTRATO, inclusive os níveis de serviços dos mesmos;
      3. teste internos e externos para assegurar o cumprimento das obrigações de acordo com a legislação e o CONTRATO firmado entre as PARTES; e
      4. aplicação de testes internos de penetração na infraestrutura ou aplicativos hospedados.
   5. O escopo das atividades de segurança deverá incluir (não se limitando a) os seguintes processos: antivírus, patches [correções] e atualizações, criptografia, configuração de novos usuários, redefinições de senhas, e exclusão ou modificação de contas de usuários. Qualquer mudança na configuração do ambiente de produção deverá obedecer ao procedimento de autorização. Quando a CONTRATADA for responsável pela configuração e/ou gestão de equipamentos, deverá informar a CONTRATANTE a configuração atual, as alterações propostas, o protocolo de testes, e os resultados dos testes. As alterações de configuração só poderão ser aplicadas após a notificação à CONTRATANTE e sua aprovação.
9. DAS FONTES DE RECURSOS
   1. As despesas decorrentes deste contrato correrão por conta dos códigos orçamentários a seguir discriminados:
      1. Unidade: 05.01.03.05
      2. Centro de Responsabilidade: 25.4.01.01.03.01.08
10. DO PRAZO DE VIGÊNCIA serviços de fornecimento contínuo
    1. O prazo de vigência do contrato será de **60 (sessenta) meses**, contados a partir da data da sua assinatura, com a possibilidade de renovação por períodos adicionais, de forma que a duração total do contrato, incluindo todas as eventuais prorrogações, não ultrapasse o limite máximo de 10 (dez) anos, desde que tais prorrogações estejam devidamente justificadas e constem do chamamento público, conforme estabelecido pela cláusula 34 do Regulamento para Contratação e Alienação (RCA).

1. DA PROPOSTA DE PREÇO
   1. A proposta de preço deve ser apresentada conforme definido abaixo:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item | Serviço | Serviço | Qtd. | Valor Mensal/Unitário (R$) | Valor Total (R$) 60 (sessenta) meses |
| 1 | Serviços de “Rede Integrada de Conectividade Empresarial” permanente, dedicados e exclusivos, de operadoras de telecomunicações distintas, baseado em infraestrutura de fibra-óptica, mediante ativação de circuito, locação de equipamentos, gerenciamento pró-ativo, solução anti-DDoS e suporte técnico 24x7, por 60 (sessenta) meses | Acesso IP Internet, com velocidade de 1 Gbps. | 3 |  |  |
| Acesso IP Internet, com velocidade de 300 Mbps. | 1 |  |  |
| Acesso IP Internet, com velocidade de 100 Mbps. | 1 |  |  |
| Acesso IP Internet, com velocidade de 50 Mbps; | 1 |  |  |
| Acesso IP Lan-to-Lan, com velocidade de 300 Mbps. | 2 |  |  |
| Microsoft Azure ExpressRoute, com velocidade de 200 Mbps. | 1 |  |  |
| Google Cloud Partner Interconnect, com velocidade de 200 Mbps. | 1 |  |  |
| Interligação Microsoft Azure ExpressRoute e Google Cloud, com velocidade de 200 Mbps. | 1 |  |  |

* 1. Nos preços apresentados devem estar inclusos todos os custos decorrentes do fornecimento do objeto deste Termo de Referência (Atendimento Comercial, Atendimento Técnico, Prevenção a ataques de negação de serviço (Anti-DDoS), Gerencia Pró Ativa, Locação Roteador), bem como todos os tributos e encargos trabalhistas, previdenciários, comerciais, além de seguros, fretes, deslocamentos de pessoal e de bens, se houverem, e quaisquer outros custos que incidam direta ou indiretamente na execução do objeto.

1. GESTÃO DO CONTRATO
   1. A gestão do contrato será realizada pela Gerência de Infraestrutura e Operações de TI da Diretoria Corporativa.
   2. A fiscalização das CONTRATANTES não exclui nem reduz a responsabilidade da CONTRATADA por quaisquer irregularidades, ainda que resultante de imperfeições técnicas, vícios redibitórios e, na ocorrência destes, não implica em corresponsabilidade das CONTRATANTES ou de seus agentes ou prepostos.