

ESPECIFICAÇÕES TÉCNICAS

1. OBJETO

Contratação de empresa para prestação de serviços de telecomunicações para a implementação, instalação, desinstalação, configuração, operação, gerenciamento, manutenção e fornecimento de link dedicado para acesso à internet por via fibra óptica, em formato full duplex - mesma velocidade de download e upload, com 100% de garantia de banda e velocidade mínima de 300 Mbps para download e 300 Mbps para upload, para a CAIXA Seguridade localizada em Brasília, pelo período de 36 (trinta e seis) meses, contados a partir da assinatura do contrato.

1.1 QUANTIDADE DO OBJETO CONTRATADO

Item	Descrição	Periodicidade do pagamento	Quantidade Estimada
1	Fornecimento de link dedicado de no mínimo 300 Mbps	Mensal	36
2	Controladora de gerenciamento	Mensal	36
3	Ativação de Pontos de Acesso Indoor	Mensal Solicitação por demanda	504
4	Serviço de instalação e configuração da solução	Único Solicitação por demanda	02
5	Serviço de desinstalação	Único Solicitação por demanda	02

2. FORMA DE EXECUÇÃO DO CONTRATO

2.1 DETALHAMENTO DA EXECUÇÃO DOS SERVIÇOS

- 2.1.1 A topologia a ser implantada deverá ser efetuada mediante ativação de circuito de comunicação de dados, comodato de equipamentos e prestação de serviços de instalação, desinstalação, configuração, suporte técnico e gerenciamento proativo de falhas conforme especificações técnicas constantes neste documento.
- 2.1.2 A CONTRATADA deverá prover o meio físico de telecomunicações para a plena utilização dos serviços contratados pela CAIXA Seguridade sem custo adicional, caso não exista, atendendo aos parâmetros definidos nas especificações, ficando este serviço sob sua inteira responsabilidade.
- 2.1.3 A alteração do meio físico para transmissão de dados por motivo de ordem técnica ou necessidade comprovada, deverá ser aprovada pela CAIXA Seguridade.
- 2.1.4 A solução adotada pela CONTRATADA deverá atender a todas as normas técnicas exigidas pelos órgãos públicos competentes e responsáveis pela regulamentação, controle e fiscalização do meio físico, da conexão lógica, do tipo de transmissão, da velocidade de tráfego, da faixa de frequência e largura de banda utilizada.

- 2.1.5 Os componentes da solução devem atender a todos os requisitos constantes neste documento.
- 2.1.6 O link deve ser dedicado e possuir velocidade mínima de 300 Mbps para upload e download por toda a vigência contratual.
- 2.1.7 A prestação do serviço compreende a instalação, desinstalação, ativação e configuração dos equipamentos necessários para a completa utilização da solução contratada.
- 2.1.8 A administração, manutenção e atualização desses equipamentos serão de inteira responsabilidade da CONTRATADA, devendo obedecer aos níveis de qualidade exigidos.
- 2.1.9 A solução deverá permitir centralizar as configurações, monitoramento e operações da rede wireless dos pontos de acesso pela CONTRATANTE.
- 2.1.10 Fornecimento de acesso à INTERNET baseado em protocolo TCP/IP IPV4. Será disponibilizado um IP válido da faixa 177.73.XX.YYY que será de uso exclusivo da CONTRATANTE durante toda a vigência do contrato.

2.1.11 **GARANTIA DE DISPONIBILIDADE**

- 2.2 A garantia de disponibilidade será de 99,9% do tempo total, em minutos, no período de 1 (um) mês.

Exemplo: 30 dias x 24 horas x 60 minutos = 43.200 x 0,1% = 43 minutos. É o tempo máximo de interrupção no período de 1 mês. Sendo ultrapassado esse tempo, será aplicada uma multa de 5% (cinco por cento) pela CAIXA Seguridade no valor mensal do contrato do mês subsequente.

3. **REQUISITOS TÉCNICOS**

3.1 **Controladora de gerenciamento**

- 3.1.1 Deve possuir estrutura que permita a instalação do equipamento em teto e parede (modelo interno) com fornecimento dos acessórios para realizar a fixação;
- 3.1.2 Deve possuir conexão Power over Ethernet (PoE);
- 3.1.3 Deve possuir velocidade wireless de no mínimo 1000 Mbps;
- 3.1.4 Deve possuir conexão RJ 45;
- 3.1.5 Deve ter capacidade de gerenciar simultaneamente no mínimo 20 (vinte) Pontos de Acesso;
- 3.1.6 Deve ter capacidade de suportar e gerenciar no mínimo 200 (duzentos) clientes conectados simultaneamente à rede WiFi;
- 3.1.7 A controladora Wi-Fi deve centralizar as configurações e operações da rede wireless de todos os pontos de acesso indoor da solução contratada;

- 3.1.8 A controladora Wi-Fi deve permitir a centralização dos parâmetros de configuração da rede wireless, políticas de segurança, QoS e sessões dos usuários, do ambiente de RF;
- 3.1.9 O acesso à controladora Wi-Fi deverá ser através de conexão segura (https) com navegador web compatível com Mozilla Firefox, Google Chrome e Microsoft Edge;
- 3.1.10 Deve possibilitar a atualização de software dos Pontos de Acesso de modo centralizado;
- 3.1.11 Deverá ter capacidade de geração de relatórios de pelo menos os seguintes tipos: Listagem de usuários conectados, Listagem de Pontos de Acesso, utilização da rede por Ponto de Acesso, detalhes de tentativas de acesso não autorizados detectados, estatísticas dos usuários/clientes;
- 3.1.12 Deve suportar backup e restauração de configurações;
- 3.1.13 Deve implementar diferentes tipos de combinações encriptação/autenticação (WPA2, WPA3 ou aberta com captive portal) por SSID;
- 3.1.14 Deve possuir recursos que possibilite visualizar a quantidade de usuários conectados em cada ponto de acesso indoor;
- 3.1.15 O equipamento deverá possuir registro na ANATEL;
- 3.1.16 Deve possuir as certificações RoHS, ISO 9001, ISO 14001 e FCC;
- 3.2 **Ponto de Acesso Indoor**
 - 3.2.1 Deve possuir estrutura que permita a instalação do equipamento em teto e parede (modelo interno) com fornecimento dos acessórios para realizar a fixação;
 - 3.2.2 Deve possuir conexão Power over Ethernet (PoE);
 - 3.2.3 Deve permitir o funcionamento simultâneo nos padrões IEEE 802.11ax em 5GHz e 2.4GHz em rede local sem fio;
 - 3.2.4 Os pontos de acesso deverão possuir certificado emitido pelo “WIFI Alliance” comprovando os seguintes padrões, protocolos e funcionalidades:
 - a. Wi-Fi CERTIFIED™ a, b, g, n, ac, 6 (ax);
 - b. WPA™ – Enterprise, Personal;
 - c. WPA2™ – Enterprise, Personal;
 - d. WPA3™ – Enterprise, Personal;
 - e. WMM®;
 - f. Deve operar com canais de 20MHz, 40MHz e 80MHz;
 - g. 802.11d e 802.11h;
 - h. WiFi 6™ - SU beamformer.
 - 3.2.5 Deve possuir as certificações RoHS, ISO 9001, ISO 14001 e FCC;

- 3.2.6 Deve possuir suporte a pelo menos 10 SSIDs com possibilidade de ativar e desativar a divulgação do SSID;
- 3.2.7 Deve permitir a criação de rede segura de convidados;
- 3.2.8 Deve possuir cliente DHCP para configuração automática de rede, sendo configurado automaticamente ao conectar na rede;
- 3.2.9 O equipamento deve possuir registro na ANATEL;
- 3.2.10 Deve possuir antenas internas omnidirecional compatíveis com as frequências de rádio dos padrões 5GHz e 2.4GHz e potência máxima de transmissão incluindo o ganho passivo das antenas de, no mínimo, 24 dBm para cada frequência;
- 3.2.11 Deve suportar pelo menos operações em 4x4 MIMO em 5Ghz e 2.4Ghz;
- 3.2.12 Deve possuir antena omnidirecional integrada com ganho de no mínimo, 3dBi em 2.4Ghz e 4dBi em 5Ghz;
- 3.2.13 Deve ser 100% compatível com a controladora de gerenciamento descrita neste documento;
- 3.2.14 Deve possuir capacidade para distribuir o sinal Wi-Fi com pelo menos 80% de intensidade em uma área de no mínimo 250 m2.

4. OBRIGAÇÕES DA CONTRATADA

4.1 INSTALAÇÃO

- 4.1.1 A Solução deverá ser ativada em sua completude em até 5 (cinco) dias úteis após a assinatura do contrato no seguinte endereço:

CAIXA SEGURIDADE
SAUS quadra 03 bloco E 3º andar
Asa Sul
70070-030 – Brasília/DF

- 4.1.2 Por solicitação da CONTRATANTE, sob demanda, a solução deverá ser desinstalada e instalada em até 5 (cinco) dias úteis no endereço abaixo:

CAIXA SEGURIDADE
SHN quadra 01 conjunto A Bloco E
Asa Norte
70701-050 – Brasília/DF

4.2 DESINSTALAÇÃO APÓS A VIGÊNCIA CONTRATUAL

- 4.2.1 Os equipamentos deverão ser removidos em 5 (cinco) dias úteis após o término contratual.

5. SEGURANÇA FÍSICA, CIBERNÉTICA E DA INFORMAÇÃO

- 5.1 Os equipamentos devem ser possuir registro na ANATEL e todas as certificações descritas no item 3.2.4 deste documento.

6. SUPORTE TÉCNICO/ATENDIMENTO

- 6.1 O atendimento de suporte será realizado por técnicos especializados, garantido 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
- 6.2 A solicitação ou necessidade de visita técnica no local será atendida em até DUAS horas, no caso de falha TOTAL no LINK, que impeça o acesso à INTERNET, com tolerância máxima de 30 (trinta) minutos. Caso a chegada no local seja superior ao tempo de 02:30h, será aplicada uma multa de 5% (cinco por cento) pela CAIXA Seguridade no pagamento mensal do contrato mês subsequente.

7. SUSTENTABILIDADE

- 7.1 Os equipamentos necessários para o pleno funcionamento do serviço devem possuir as certificações RoHS, ISO 9001, ISO 14001 e FCC.
- 7.1.1 Estas certificações devem ser entregues na fase de habilitação juntamente com a apresentação do atestado de qualificação técnica.

8. CLÁUSULAS DE PRIVACIDADE E SEGURANÇA DAS INFORMAÇÕES

- 8.1 Esta contratação é classificada como grau de criticidade baixo.
- 8.2 Esta contratação não tem como escopo o tratamento de dados pessoais;
- 8.3 A CONTRATADA deve conhecer e cumprir a Política de Segurança e Informação da CAIXA, disponibilizada no site da CAIXA (<https://www.caixa.gov.br/Downloads/caixa-governanca/politica-seguranca-informacao.pdf>), e CAIXA Seguridade (<https://www.ri.caixaseguridade.com.br/governanca-corporativa/estatuto-politicas-e-codigos/>), dando conhecimento aos seus funcionários no âmbito da prestação dos serviços objeto do contrato.
- 8.4 Os fornecedores devem cumprir todos os requisitos da legislação brasileira aplicáveis à segurança da informação e privacidade de dados, bem como devem se comprometer integralmente à observância dos itens a seguir:
- 8.4.1 Conhecer e cumprir a Política de Segurança e Informação da CAIXA Seguridade;
- 8.4.2 Proteger as informações corporativas e de clientes da CAIXA Seguridade contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade;
- 8.4.3 Garantir que seus empregados e colaboradores tratem de forma estritamente confidencial todas as informações levadas a seu conhecimento pela CAIXA Seguridade durante a prestação dos serviços ou em função deles e somente as utilizarão no âmbito dos serviços contratados;

- 8.4.4 Garantir que seus empregados e colaboradores respeitem os ambientes físicos e demais locais sinalizados como área restrita, cumprindo todas as definições e proibições de registros fotográficos, gravações de áudio, vídeo, bem como as restrições de compartilhamento desses materiais em qualquer mídia ou rede social;
- 8.4.5 Garantir que seus empregados e colaboradores sejam periodicamente sensibilizados e conscientizados em relação à segurança da informação, à privacidade e à proteção de dados pessoais;
- 8.4.6 Garantir que as práticas de segurança da informação por eles executadas sejam divulgadas e exigidas de todos os componentes de sua cadeia de suprimento;
- 8.4.7 Assegurar que os recursos e informações colocados à sua disposição sejam utilizados apenas para as finalidades contratadas;
- 8.4.8 Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- 8.4.9 Garantir a continuidade do processamento das informações críticas de negócios;
- 8.4.10 Cumprir as Leis e normas que regulamentam a propriedade intelectual e direitos autorais;
- 8.4.11 Atender às Leis que regulamentam a atividade da CAIXA Seguridade e seu mercado de atuação;
- 8.4.12 Comunicar imediatamente à CAIXA Seguridade qualquer descumprimento destas diretrizes.
- 8.5 Estas diretrizes de segurança e privacidade se aplicam aos fornecedores de bens e serviços contratados pela CAIXA Seguridade, incluindo seus sócios, administradores, diretores, empregados, prepostos, contratados, consultores, ou quaisquer outras pessoas sob sua responsabilidade (direta ou indireta), que venham a ter acesso a ambientes, sistemas e informações da CAIXA Seguridade.

9. CLÁUSULAS DE SEGURANÇA CIBERNÉTICA PARA FORNECEDORES

- 9.1 Não se aplica, uma vez que não haverá tratamento de dados da CAIXA e/ou CAIXA Seguridade.