Secretaria de Finanças e Planejamento
06
SEFIN

PROCESSO ADMINISTRATIVO

TERMO DE REFERÊNCIA

SECRETARIA DE FINANÇAS, PLANEJAMENTO E ORÇAMENTO DE CAUCAIA

2. DO OBJETO

2.1. O objeto deste Termo de Referência é a aquisição de solução de rede com serviço de instalação, configuração, suporte técnico para 06 meses e garantia do fabricante para 12 meses.

3. DA DESCRIÇÃO DETALHADA DA SOLUÇÃO

3.1. Esta solução contempla os equipamentos e serviços necessários para interconectividade sem fio aos serviços atualmente existentes da Secretaria de Finanças, Planejamento e Orçamento da Prefeitura de Caucaia.

3.1.1 PONTO DE ACESSO 802.11ac WAVE 2 DUAL-BAND INDOOR:

3.1.1.1. Especificações Gerais:

a) Deverá ser do mesmo fabricante do controlador WLAN.

b) Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

c) Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point.

d) Deve ser compatível com o padrão UL 2043, a qual regula os componentes dos materiais com o

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

intuito de proteger contra danos causados por fogo, bem como pela fumaça.

e) Suportar, no mínimo, 255 (duzentos e cinquenta e cinco) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

f) Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

g) Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3af ou 802.3at).

h) Deve suportar temperatura de operação entre 0°C a 40°C.

i) Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

j) O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

k) Deve possuir LEDs para a indicação do status das portas ethernet, rede wireless, gerenciamento via controladora e da atividade do equipamento.

l) Deverá ser fornecido com todas as funcionalidades de segurança habilitadas, incluindo WIPS/WIDS.

m) Deverá ser fornecido com a versão mais recente de software.

n) Deverá ser novo, de primeiro uso, e estar na linha de produção atual do fabricante.

3.1.1.2. Características dos Rádios:

a) O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac Wave 1 e Wave 2, com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea.

b) Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 11, 5.5, 2 e 1 Mbps, IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps, IEEE 802.11n: 6.5 Mbps a 300 Mbps e IEEE 802.11ac: 6.5 Mbps a 867 Mbps.

c) Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac, com ganhos de, no mínimo, 3 dBi para 5 GHz.

d) Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 23 dBm nas frequências de 5GHz e 2.4GHz.

e) Deverá suportar canalização de 20MHz, 40MHz e 80MHz.

f) Deverá possuir mecanismo de rádio com suporte a SU-MIMO e MU-MIMO 2x2 com 2 fluxos espaciais.

g) Deve possuir sensibilidade mínima de recepção de -91dBm considerando MCS0 VHT20 (802.11ac) em 5GHz e -91dBm MCS0 HT20 (802.11n) em 2.4GHz.

h) Deve possuir suporte a RTS com sinalização de bandwidth em 802.11ac, o qual deve ser devidamente comprovado mediante certificado da WiFi Alliance, órgão imparcial e independente.

i) Deve ser compatível com 802.11ac MU-MIMO e suportar transmissão no sentido downlink, ou seja, do ponto de acesso para o dispositivo do usuário final, sendo que este item deve ser devidamente comprovado mediante certificado da WiFi Alliance, órgão imparcial e independente.

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

j) Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

k) Possuir capacidade de selecionar automaticamente o canal de transmissão.

l) Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

3.1.1.3. Rede de Serviços:

a) Deve ser compatível com IPv4 e IPv6.

b) Deverá possuir 01 (uma) interface 10/100/1000 Mbps Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa.

c) Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

d) Deve suportar, em conjunto com o controlador de rede sem fio, a configuração de limite de banda por usuário ou por SSID.

e) Deve oferecer suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service).

f) O ponto de acesso poderá estar conectado diretamente ou remotamente ao controlador WLAN, inclusive através de roteamento em Camada 3 do modelo OSI.

g) Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora.

h) Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

i) Deve suportar VLANs conforme o padrão IEEE 802.1Q.

j) Deve suportar atribuição dinâmica de VLAN por usuário.

k) Deve implementar balanceamento de usuários por ponto de acesso.

l) Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

m) Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

n) Deve suportar conversão de tráfego multicast para unicast.

3.1.2. Segurança e Gerenciamento:

a) Deve suportar a utilização de sistema antifurto do tipo Kensington lock ou similar que permita a instalação de um cabo de segurança com a finalidade de evitar furto do equipamento.

b) Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, DPSK, IEEE 802.1X e IEEE 802.11i.

c) Deverá permitir a criação de filtros de endereço MAC de modo a restringir o acesso à rede sem fio.

d) Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

e) Deverá ser possível criar políticas de controle com base no tipo de sistema operacional ou do dispositivo.

f) Permitir habilitar e desabilitar a divulgação do SSID.

g) Deve implementar autenticação de usuários usando portal de captura (captive portal).

h) Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

i) Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através do controlador, a fim de se garantir a segurança dos dados.

j) Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento da rádio frequência.

k) Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

l) Permitir que o processo de atualização de software seja realizado manualmente através de interface web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

3.2. GERENCIAMENTO DA REDE WLAN

3.2.1. Características Gerais:

3.2.1.1. Deverá ser compatível com pontos de acesso internos e externos nos padrões 802.11ac Wave 2 e 802.11ax.

3.2.1.2. Capacidade para gerenciar, no mínimo, 128 (cento e vinte oito) Pontos de Acesso.

3.2.1.3. Suportar, no mínimo, 2000 (dois mil) dispositivos simultâneos.

3.2.1.4. Prover o gerenciamento centralizado dos Pontos de Acesso do mesmo fabricante para fins de compatibilidade.

3.2.1.5. Permitir o funcionamento e gerenciamento sem a necessidade de controlador WLAN dedicado, seja por meio de appliance físico ou máquina virtual ou controlador em nuvem, onde, dessa forma, os pontos de acesso atuam de modo autônomo e são gerenciados por um ponto de acesso eleito como o principal em um grupo de atuação.

3.2.1.6. Deve ser possível definir quais pontos de acesso serão designados como principal e secundário.

3.2.1.7. Esta solução deverá apresentar uma gerência através de padrão WEB, que deverá permitir a realização da configuração total dos pontos de acesso, incluindo seus parâmetros wireless, políticas de segurança, autenticação e monitoramento de rádio frequência, necessárias para a operação da rede sem fio.

3.2.1.8. Deve suportar o idioma da interface Web para português do Brasil.

3.2.1.9. Deve suportar o agrupamento de pontos de acesso em grupos de APs distintos.

3.2.1.10. Deve automaticamente propagar um SSID por padrão para que seja possível realizar a configuração inicial por meio de um navegador Web e uma instalação guiada.

3.2.1.11. Possibilitar a configuração de envio dos eventos para um servidor Syslog remoto.

3.2.1.12. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP.

3.2.1.13. Permitir a visualização de alertas da rede via interface Web.

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

3.2.1.14. Implementar, pelo menos, protocolo de autenticação para controle do acesso administrativo ao equipamento através de autenticação local (Local Authentication Database) e autenticação externa (RADIUS e Active Directory).

3.2.1.15. Implementar, no mínimo, 2 (dois) níveis de acesso administrativo (apenas leitura e leitura/escrita) protegidos por senhas independentes.

3.2.1.16. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS).

3.2.1.17. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou FTP ou TFTP.

3.2.1.18. Deverá implementar disponibilidade de SSID baseado em dia da semana/hora, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia da semana determinados.

3.2.1.19. Deve ser possível definir a prioridade do SSID, onde um SSID corporativo será mais prioritário que um SSID visitante.

3.2.1.20. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível (ping, trace e logs).

3.2.1.21. Possibilitar cópia "backup" da configuração, bem como a funcionalidade de restauração da configuração através de browser padrão (HTTPS) ou FTP ou TFTP.

3.2.1.22. Suportar redundância na existência de 2 (duas) unidades, no modo ativo/ativo ou ativo/standby, com sincronismo automático das configurações entre unidades.

3.2.1.23. O gerenciamento deverá ser realizado através de um único endereço IP.

3.2.1.24. Em caso de falha, a redundância deverá ser realizada de forma automática sem nenhuma ação do administrador de rede.

3.2.1.25. Deverá possuir painéis demonstrando informações dos seguintes tipos: Listagem de clientes sem fio, incluindo informações de endereço IP, endereço mac, sistema operacional, nível de sinal, método de autenticação, rede sem fio, nome do AP, bem como Listagem de Pontos de Acesso, utilização da rede, detalhes dos pontos de acesso não autorizados (rogues) detectados.

3.2.1.26. Deve suportar, somente por meio do ponto de acesso, sem necessidade de ferramenta adicional, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

3.2.1.27. Deve suportar até 500 (quinhentos) usuários locais na base de dados interna.

3.2.2. Rede

3.2.2.1. Deverá possuir servidor DHCP embutido.

3.2.2.2. Deverá implementar tagging de VLANs através do protocolo 802.1q

3.2.2.3. Deverá oferecer os recursos de mobilidade para roaming de camada L2.

3.2.2.4. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X.

3.2.2.5. Deverá suportar, no mínimo, 16 (dezesseis) SSIDs simultâneos.

3.2.2.6. Deve ser possível desconectar o cliente caso o mesmo não obtenha endereço IP via DHCP.

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

3.2.3. Segurança

3.2.3.1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação.

3.2.3.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

a) (WPA) Wi-Fi Protected Access.

b) (WPA2) Wi-Fi Protected Access 2.

c) (WPA3) Wi-Fi Protected Access 3.

d) (AES) Advanced Encryption Standard.

e) IEEE 802.1X.

3.2.3.3. Implementar, pelo menos, os seguintes controles/filtros:

a) L2 – Baseado em endereço MAC e Client Isolation.

b) L3 – Baseado em Endereço IP.

c) L4 – Baseado em Portas TCP/UDP.

d) Baseado em Tipo ou Sistema Operacional do dispositivo.

3.2.3.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

a) MAC Address.

b) Autenticação Local.

c) Captive Portal.

d) Active Directory.

e) RADIUS.

f) IEEE 802.1X.

3.2.3.5. Deverá permitir que a autenticação de usuários seja executada através da utilização de credenciais de acesso a mídias sociais com suporte a, no mínimo, Facebook, Google e LinkedIn.

3.2.3.6. Deverá permitir a seleção/uso de servidor Radius ou Active Directory específico com base no SSID.

3.2.3.7. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

3.2.3.8. A solução deverá suportar a criação de uma zona de visitantes, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso à rede wireless.

3.2.3.9. Deverá permitir a criação de múltiplos usuários visitantes de uma única vez, ou seja, em lote.

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

3.2.3.10. Deve ser possível criar um usuário específico com autorização para geração de senhas individuais de visitantes.

3.2.3.11. Deve permitir que após o processo de autenticação de usuários visitantes, os mesmos sejam redirecionados para uma página de navegação específica e configurável.

3.2.3.12. Deve permitir que o portal interno para usuários visitantes seja customizável.

3.2.3.13. Deve permitir que múltiplos usuários visitantes compartilhem a mesma senha de acesso à rede.

3.2.3.14. Deverá permitir que os usuários façam um simples cadastro no sistema, preenchendo as informações solicitadas e obtenham acesso à rede de visitantes.

3.2.3.15. Deverá permitir enviar a senha de usuários visitantes, por e-mail ou por SMS.

3.2.3.16. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa.

3.2.3.17. Implementar, mecanismos para detecção de pontos de acesso do tipo rogue com informações de no mínimo:

3.2.3.17.1. SSID-Spoofing – APs não pertencentes a solução propagando o mesmo SSID.

3.2.3.17.2. MAC Spoofing – APs não pertencentes a solução propagando o mesmo MAC de um AP válido.

3.2.3.17.3. Rogue DHCP Server.

3.2.3.18. Deve implementar varredura de rádio frequência nas bandas de 2.4GHz e 5GHz para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues).

3.2.3.19. Deve ser possível classificar um ponto de acesso do tipo rogue como malicioso.

3.2.3.20. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN.

3.2.3.21. Deve utilizar os Pontos de Acesso para fazer o monitoramento do ambiente sem fio procurando por pontos de acesso do tipo rogue de forma automática.

3.2.3.22. Deve suportar filtro ARP para minimizar ou limitar a quantidade de broadcast ARP.

3.2.4. Recursos de gerenciamento automático de rádio frequência:

3.2.4.1. Implementar varredura de rádio frequência contínua com identificação de Pontos de Acesso irregulares, tal como rogue.

3.2.4.2. Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida.

3.2.4.3. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de rádio frequência.

3.2.4.4. Detectar interferência e ajustar parâmetros de rádio frequência, evitando problemas de cobertura de modo automático.

3.2.4.5. Ajustar dinamicamente o nível de potência e canal de rádio dos Pontos de Acesso, de modo a otimizar o tamanho da célula de rádio frequência, garantindo o desempenho e escalabilidade.

3.2.4.6. Implementar sistema automático de balanceamento de carga para associação de clientes

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

entre Pontos de Acesso próximos, para otimizar o desempenho.

3.2.4.7. Suportar 802.11d, 802.11k e 802.11r.

3.2.4.8. Deve suportar CAC (Call Admission Control).

3.2.4.9. Deve suportar limite de banda por SSID ou por estação.

3.2.4.10. Deve possuir suporte a Bonjour.

3.2.5. Recursos de convergência e multimídia:

3.2.5.1. Deverá possuir funcionalidade de configuração do limite de banda disponível por estação ou por SSID, mas ambas opções devem estar disponíveis.

3.2.5.2. Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como VoIP, VoWLAN e videoconferência.

3.3. SERVIÇO DE INSTALAÇÃO DA SOLUÇÃO WLAN:

3.3.1. A entrega, a instalação e a configuração dos equipamentos e softwares serão de inteira responsabilidade da CONTRATADA.

3.3.2. A instalação deverá contemplar, no mínimo, as seguintes etapas.

3.3.3. Definição da topologia, segmentação e endereçamento das WLANs.

3.3.4. Configurar os SSIDs (Locais e Visitantes) para as redes conforme planejamento estabelecido pela CONTRATANTE.

3.3.5. Definir políticas de bloqueio e permissão de acessos à rede Wifi.

3.3.6. A rede de visitante (guest) deverá encaminhar o trafego de internet através de servidores e topologia de rede definidos em conjunto com a equipe de TI da SEFIN.

3.3.7. Configuração de Endereços/Interfaces de Gerencia.

3.3.8. Configuração de algoritmo de criptografia, métodos de autenticação e segurança a serem utilizados.

3.3.9. Configuração do captive portal de autenticação (portal cativo).

3.3.10. Testes de funcionamento do ambiente integrado de WLAN.

3.3.11. O teste de funcionamento do ambiente integrado de WLAN deve ser realizado com pontos de acesso instalados em pelo menos um pavimento das instalações da CONTRATANTE, de forma a demonstrar o funcionamento integrado da WLAN.

3.4. SERVIÇO DE SUPORTE TÉCNICO DA SOLUÇÃO WLAN:

3.4.1. Após a implantação a CONTRATADA deverá prestar suporte técnico, sob demanda, em horário comercial, para acompanhamento e aperfeiçoamento do funcionamento da solução.

3.4.2. O suporte técnico deverá ser prestado na modalidade remota, com o uso de software de acesso remoto seguro.

3.4.3. O suporte técnico poderá ser prestado nas dependências da SEFIN, de acordo com calendário a ser definido pelo cliente.

3.4.4. Os prazos de atendimento serão os seguintes:

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004

3.4.5. Normais: Início de atendimento em até 04 (quatro) horas e solução em 02 (dois) dias úteis a contar da data e hora de abertura do chamado;

3.4.6. Urgentes: Início de atendimento em até 01 (uma) hora e solução em até 04 (quatro) horas úteis a contar da data e hora de abertura do chamado;

3.4.7. Entende-se por horário útil, o horário compreendido entre as 08h00min e 18h00min, de segunda à sexta-feira, exceto em feriados no município de Caucaia.

4. DOS PREÇOS E PAGAMENTO

4.1. O preço deverá estar indicado em moeda nacional, incluídas quaisquer vantagens, abatimentos, impostos, taxas e contribuições sociais, obrigações trabalhistas, previdenciárias, fiscais e comerciais, que eventualmente incidam sobre a operação; ou, ainda, despesas com transporte ou terceiros, que correrão por conta da CONTRATADA;

4.2. Deverá ser apresentado segundo a Tabela 1:

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Equipamento Access Point	03	R$	R$
2	Serviço de Instalação e Configuração	01	R$	R$
3	Serviço de Suporte Técnico para 06 meses	01	R$	R$
			VALOR TOTAL	**R$**

Tabela 1

4.3. O pagamento do ITEM 1 ocorrerá em até 10 (dez) dias corridos após a entrega dos equipamentos, mediante a apresentação do documento fiscal de cobrança, conferido e atestado pelo Gestor do Contrato;

4.4. O pagamento dos ITENS 2 e 3 ocorrerá em até 10 (dez) dias corridos após a conclusão do serviço de instalação dos equipamentos, mediante a apresentação do documento fiscal de cobrança, conferido e atestado pelo Gestor do Contrato.

Caucaia, 19 de JULHO de 2021.

George Veras Bandeira
Secretário de Finanças, Planejamento e Orçamento.

Rua Coronel Correia, 1767
Centro, Caucaia – CE
CEP. 61600-004