Termo de Referência

Contratação de Solução de Autenticação e Gerenciamento de Conexões Wi-Fi
Elaborada exclusivamente para a PROCEMPA junto ao SEI 25.12.000001248-0
Validade: de 09/10/2025 até 09/10/2026

ESPECIFICAÇÃO TÉCNICA

1. OBJETO

1.1. Contratação de Solução de Autenticação e Gerenciamento de Conexões Wi-Fi, com serviço de subscrição (subscription) para suporte técnico e atualizações, a ser instalada em ambiente computacional virtual próprio da Procempa (modelo on-premises).

2. A CONTRATAÇÃO CONTEMPLA

2.1. O fornecimento da Solução completa para instalação no datacenter da Procempa.

2.2. Serviços de implantação, configuração e treinamento da equipe técnica.

2.3. Um plano de subscrição anual que garanta suporte técnico especializado e acesso a todas as atualizações de versão (correções de bugs, correções de segurança e novas funcionalidades) do software.

HABILITAÇÃO TÉCNICA

3. MODELO DE LICENCIAMENTO E ESCALABILIDADE

3.1. O modelo de licenciamento e remuneração deverá ser baseado no número de access points (APs) ativos na plataforma.

3.2. O volume inicial de APs é de 1.800 dispositivos, com possibilidade de expansão anual de até 15% em relação à base inicial. Independentemente desta estimativa, a Solução ofertada deverá ser concebida com arquitetura robusta e escalável, capaz de ser flexível para suportar volumes de dispositivos superiores ao previsto, garantindo as funcionalidades e performance de todas as funcionalidades.

3.3. A Solução deve ser agnóstica ao hardware de rede dos APs, com compatibilidade comprovada com os fabricantes Aerohive, Ruckus, TP-Link e UniFi e suas respectivas controladoras WLAN: Extreme CloudIQ Pilot v.21.1.23.4, Ruckus SmartZone v.6.1.2, TP-Link Omada v.5.15 e UniFi v.9.2.

4. ENTREGA DA SOLUÇÃO

4.1. A Solução deverá ser entregue como appliance virtual ou em formato compatível para instalação em ambiente VMware vSphere versão 8.

4.2. A CONTRATADA será responsável pela instalação, configuração e ativação de todos os subsistemas, módulos e integrações, deixando a Solução em perfeito funcionamento.

4.3. Deve ser compatível com a arquitetura atual da Procempa, que utiliza gateways CGNAT para os clientes de Wi-Fi e rede de gerência apartados.

4.4. A arquitetura da Solução está sujeita à análise de riscos e à validação da equipe de Segurança da Informação da Procempa.

5. PLATAFORMA DE GERENCIAMENTO CENTRALIZADO

5.1. O software de gerenciamento deverá disponibilizar painel(is) de controle (dashboard) acessível(is) via interface web, em língua portuguesa (Brasil), com funcionalidades configuráveis e dinâmicas.

5.2. Deve permitir a gestão centralizada de cadastro e segurança de todos os APs.

5.3. Deve possuir arquitetura multi-tenant, com segregação lógica de localidades e perfis de administração, com diferentes níveis de permissão.

5.4. A Solução deverá possuir mecanismos de monitoramento do serviço em regime 24x7, com suporte a protocolos de gerenciamento e monitoração de rede, como SNMP (v2/v3) e/ou APIs, permitindo integração com ferramentas de NOC/SOC (Zabbix) da Procempa.

5.5. Deve possuir controle de acesso de administrador por usuário e grupo no AD (Active Directory).

5.6. A Solução deverá ser implementada em uma arquitetura de cluster, garantindo alta disponibilidade e escalabilidade horizontal.

6. CAPTIVE PORTAL (PORTAL DE AUTENTICAÇÃO)

6.1. Deve possuir editor flexível e personalizável, com interface amigável para criação e personalização do portal, alternativamente, permitindo também edições avançadas por meio de HTML, CSS e JavaScript.

6.2. Deve possuir habilitação automática de idioma (mínimo: português e inglês).

6.3. Métodos de autenticação suportados:

6.3.1. Acesso corporativo: integração nativa com Microsoft Active Directory (AD) e/ou LDAP.

6.3.2. Acesso de visitantes: redes sociais, plataforma GOV.BR, formulários personalizáveis e protocolos abertos como: OAuth 2.0 e OpenID Connect (OIDC).

6.4. Deve possuir funcionalidade whitelabel (URL customizada), permitindo identificar na página de autenticação a identidade visual e endereço da própria instituição.

7. CONTROLE DE ACESSO E POLÍTICAS DE REDE

7.1. Deve possuir capacidade de gerar cadastro próprio, com validação de CPF e confirmação do cadastro por telefone (via SMS) e e-mail (via link de verificação).

7.2. Deve possuir capacidade de recursos adicionais, a serem processadas previamente a liberação da autenticação, como: realização e captura de respostas de pesquisas de opinião, exibição de vídeos, campanhas com banners/cards, enquetes condicionais e termos de uso customizáveis. A Solução deverá possuir funcionalidades para o controle granular de acesso por usuário ou por grupo de usuários, contemplando, no mínimo, as seguintes políticas:

7.2.1. Controle de Tempo de Conexão: com limite por sessão para definir a duração máxima de uma única sessão de conexão contínua.

7.2.2. Cota de Tempo Agregado: para definir uma cota total de tempo de uso por dia, semana ou mês.

7.2.3. Programação de Janela de Acesso: para restringir o acesso à rede a dias e horários específicos.

7.3. Deve permitir definir de limites de acesso e políticas personalizadas.
7.4. Deve garantir restrição para não permitir múltiplos cadastros com o mesmo CPF ou e-mail.
7.5. Deve possibilitar bloqueio de usuários e dispositivos, com possibilidade de cadastro manual de dispositivos/usuários.

8. LOGS

8.1. Deve ter opção para garantir armazenamento seguro e inviolável de logs de conexão por, no mínimo, 1 ano.
8.2. A Solução deverá permitir a exportação de logs para sistemas externos, como servidores de banco de dados ou plataformas de centralização de logs.
8.3. Deve ter opção de manter registros obrigatórios por sessão: usuário (CPF), IP, MAC address, data/hora de início/fim e AP utilizado.

9. RELATÓRIOS

9.1. Deve permitir gerar relatórios com histórico de acessos, de visitantes únicos ou recorrentes.
9.2. Deve permitir gerar relatórios com registros de tempo médio de conexão, tráfego total (download/upload).
9.3. Deve permitir gerar relatórios com mapas de calor e fluxo de pessoas por AP.
9.4. Deve permitir gerar relatórios com rankings de usuários por tempo e volume de tráfego.
9.5. Deve permitir gerar relatórios com resultados de campanhas visualizadas e interações.
9.6. Deve permitir gerar relatórios exportáveis nos formatos: CSV, XLS e PDF.
9.7. Deve permitir segregar tráfego de visitantes e funcionários.
9.8. Deve permitir emitir relatórios de presença: tempo de permanência, frequência e recorrência.

10. INTEGRAÇÕES E APIS

10.1. Deve possuir APIs robustas para importação e exportação de dados.
10.2. Deve possuir integração com BI, SGBDs e webhooks.
10.3. Deve permitir envio automatizado de comunicações (e-mail, SMS) baseadas em cadastros ou gatilhos de comportamento.

11. CONFORMIDADE E SEGURANÇA

11.1. Deve estar em conformidade com o Marco Civil da Internet (Lei nº 12.965/2014) e LGPD (Lei nº 13.709/2018).
11.2. Deve suportar autenticação e accounting via RADIUS (com redundância e CoA).
11.3. Deve suportar cadastro por vouchers e autosserviço (self-registration).

Termo de Referência

Contratação de Solução de Autenticação e Gerenciamento de Conexões Wi-Fi
Elaborada exclusivamente para a PROCEMPA junto ao SEI 25.12.000001248-0
Validade: de 09/10/2025 até 09/10/2026

12. TREINAMENTO E SUPORTE

12.1. Deve ofertar treinamento técnico para, no mínimo, 6 (seis) analistas da Procempa.

12.2. Deve assegurar suporte técnico especializado para a Solução, em português, 8x5 (questões gerais) e 24x7 (indisponibilidade crítica).

12.3. As atualizações de software (patches releases, security patches e novas versões) serão incluídas sem custo adicional, durante a vigência da contratação.

Obrigações da Contratada

13. Fornecer, instalar, configurar e deixar em pleno funcionamento a Solução de autenticação e gerenciamento de conexões Wi-Fi, em ambiente computacional da Procempa.
14. Assegurar suporte técnico especializado em português, no regime 8x5 para demandas gerais e 24x7 para indisponibilidades críticas, com atualizações de software incluídas durante toda a vigência contratual.
15. Assegurar que a Solução estejam em conformidade com o Marco Civil da Internet e com a LGPD, assegurando armazenamento seguro e inviolável dos registros obrigatórios.
16. Assegurar compatibilidade da Solução com os fabricantes e controladoras especificadas, bem como com os recursos de Captive Portal, políticas de acesso e relatórios de monitoramento.
17. Disponibilizar treinamento técnico para operação e administração da plataforma

Critérios de Aceite

18. No prazo de até 15 (quinze) dias antes da assinatura do contrato, a LICITANTE deverá disponibilizar ambiente de teste funcional para comprovar a conformidade da Solução com os fabricantes e controladoras WLAN informadas abaixo. O serviço será considerado aceito após a validação de comunicação e autenticação de rádios wi-fi com as seguintes fabricantes e controladoras:

18.1. Extreme CloudIQ Pilot v.21.1.23.4.

18.2. Ruckus SmartZone v.6.1.2.

18.3. TP-Link Omada v.5.15.

18.4. UniFi v.9.2 .

19. O êxito nos testes de compatibilidade descritos no item 17 é condição indispensável e eliminatória para o prosseguimento da contratação. A falha em comprovar a interoperabilidade da Solução nos ambientes listados resultará na desclassificação da proposta da LICITANTE.

20. A Solução deverá ser entregue, instalada, configurada e ativada no ambiente da Procempa, em pleno funcionamento e conforme as especificações do Termo de Referência.

21. Validação do funcionamento do Captive Portal, com suporte a métodos de autenticação exigidos (AD/LDAP, redes sociais, GOV.BR, formulários, OAuth 2.0, OIDC).
22. Verificação do armazenamento seguro e inviolável de logs de conexão, com todos os registros obrigatórios (CPF, IP, MAC, data/hora, AP utilizado).
23. Testes de emissão de relatórios e de relatórios exportáveis (CSV, XLS, PDF), incluindo acessos, tráfego, visitantes, rankings e mapas de calor.
24. Funcionamento e operacionalização dos mecanismos de monitoramento contínuo (24x7), com integração SNMP e/ou API com ferramentas de NOC/SOC da Procempa.
25. Informação da disponibilização de canal de suporte técnico especializado, em português, conforme os regimes definidos (8x5 para demandas gerais e 24x7 para indisponibilidades críticas).
26. Entrega de treinamento técnico da Solução.
27. Entrega de declaração formal de conformidade com o Marco Civil da Internet (Lei nº 12.965/2014) e a LGPD (Lei nº 13.709/2018).
28. O aceite final da Solução será concedido após a comprovação de seu pleno funcionamento em nosso ambiente produtivo, a efetiva capacitação de nossa equipe técnica para sua administração e operação, com a entrega e aprovação da documentação técnica completa. Esta documentação deve ser suficiente para garantir nossa autonomia na gestão da plataforma, detalhando os procedimentos de instalação, configuração, operação diária e, fundamentalmente, as rotinas de administração da ferramenta.

Vigência

29. O contrato terá vigência de 12 (doze) meses, podendo ser renovado por mais 48 (quarenta e oito) meses.

Prazo de Entrega

30. A Solução deverá ser entregue: instalada, configura e funcional, em até 30 dias após a assinatura do contrato.