CONSULTA PRELIMINAR AO MERCADO DAG/DIRS N.º 21/2024

Equipamentos de Wi-Fi

Nota legal:

Esta apresentação é apenas uma versão preliminar do projeto pretendido, partilhada apenas para fins de informação geral, não podendo ser considerada versão final, nem vinculativa.

As informações contidas neste documento podem estar sujeitas a alterações, não comprometendo nem vinculando os Serviços Partilhados do Ministério da Saúde, EPE e/ou quaisquer outros serviços e/ou órgãos do Ministério da Saúde ou do Serviço Nacional de Saúde.

I. ENQUADRAMENTO

A SPMS tem por missão a prestação de serviços partilhados nas áreas de compras e logística, serviços financeiros, recursos humanos e sistemas e tecnologias de informação e comunicação às entidades com atividade especifica na área da saúde, de forma a "*centralizar, otimizar e racionalizar*" a aquisição de bens e serviços no Serviço Nacional de Saúde.

Os Sistemas de Informação na Saúde permitem a cooperação, a partilha de conhecimentos e informação, bem como o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas e tecnologias de informação e comunicação. Desempenham um papel importante na reforma do sistema de saúde, tendo como principais objetivos a melhoria da acessibilidade, eficiência, qualidade e continuidade dos cuidados e o aumento da satisfação dos profissionais e cidadãos.

À SPMS cabe, ainda, a garantia da operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde, promovendo a definição e a utilização de normas, metodologias e requisitos que garantam a interoperabilidade e interconexão dos sistemas de informação da saúde entre si, e com os sistemas de informação transversais à Administração Pública, visando desenvolver e proteger a saúde dos cidadãos.

II. OBJETIVO

Pretende assim a SPMS, EPE vir a adquirir equipamentos, serviços de levantamento de requisitos, instalação e configuração para a modernização da infraestrutura Wi-Fi. O objetivo é aprimorar a cobertura do sinal, a

segurança, a alta disponibilidade e a resiliência da solução. Com vista à preparação do respetivo procedimento aquisitivo, e fazendo uso do disposto no artigo 35.º-A do Código dos Contratos Públicos, a SPMS, EPE vem, nos termos da denominada "consulta preliminar ao mercado", solicitar informações sobre o objeto do contrato.

Assim, na presente consulta preliminar ao mercado, pretende-se identificar:

1. O preço base a considerar pela entidade adjudicante face aos equipamentos pretendidos;
2. O preço base a considerar pela entidade adjudicante para os serviços de pré-instalação dos componentes passivos de rede, quanto a instalação e configuração de todos os sistemas ativos que compõem a solução;
3. Análise da viabilidade para os operadores económicos do procedimento, alocar os equipamentos a um adjudicatário, e os serviços a adjudicatário diferente;
4. Prazo considerado necessário para a entrega dos equipamentos e informação da necessidade de entregas faseadas;
5. Prazo considerado necessário para a instalação e configuração dos equipamentos.

III. OBJECTO DA CONSULTA

Tendo por base os pressupostos anteriores, a consulta preliminar será constituída por:

1. **Pontos de Acesso Wireless (AP's)**
2. **Cluster de Controladoras Wireless – Tipo 1 e 2**
3. **Componente de Controlo de Acesso à Rede (NAC) e Sistemas Associados – Tipo 1 e 2**
4. **Serviços de levantamento de Requisitos**
5. **Serviços de Instalação e Configuração de todas as componentes a concurso**
6. **Serviços de Assistência Técnica Preventiva e Corretiva durante o período de 36 meses com cobertura 24 x 7 com 4h de tempo de resposta para os equipamentos referidos em a)**
7. **Serviços de Operacionalização Técnica durante o período de 36 meses para os equipamentos ou software referidos em b) e c)**

Equipamentos e clusters de *appliances* físicas a adquirir – Tipo 1

Requisitos mínimos			
Ponto	Descrição		Quantidade
I	**Pontos de Acesso Wireless (AP's)**		10 000
Ponto	Descrição	Nº de clusters	Nº de nós (por cluster)
ii	**Cluster de Controladoras Wireless**	>= 3	>= 3
iii	**Cluster de Appliances para Gestão de Acesso à Rede (NAC) e Sistemas Associados**	>= 3	>= 2
Ponto	Descrição		Quantidade
iv	**Serviços de Assistência Técnica Preventiva e Corretiva o período de 36 meses com cobertura 24 x 7 com 4h de tempo de resposta, - valores separados para o ponto: i**		1
v	**g) Serviços de Operacionalização Técnica durante o período de 36 meses para os equipamentos ou software referidos- valores separados para os pontos: ii, iii, e iv**		1

Equipamentos e *appliances* virtuais a adquirir – Tipo 2

Requisitos mínimos				
Ponto	Descrição			Quantidade
I	**Pontos de Acesso Wireless (AP's)**			10 000
Ponto	Descrição	Nº de clusters	Nº de nós (por cluster)	Nº Instâncias (por nó)
ii	**Cluster de Controladoras Wireless**	>= 3	>= 3	>= 3
iii	**Cluster de Appliances para Gestão de Acesso à Rede (NAC) e Sistemas Associados**	>= 3	>= 3	>= 3
Ponto	Descrição			Quantidade
iv	**Serviços de Assistência Técnica Preventiva e Corretiva o período de 36 meses com cobertura 24 x 7 com 4h de tempo de resposta, - valores separados para o ponto: i**			1
v	**g) Serviços de Operacionalização Técnica durante o período de 36 meses para os equipamentos ou software referidos- valores separados para os pontos: ii, iii, e iv**			1

a) Cumprir as alíneas a) a g) do n.º 5 da Deliberação n.º 1/2023 da Comissão de Avaliação de Segurança, disponível em https://www.gns.gov.pt/docs/cas-1-2023.pdf.

3.1. PRESSUPOSTOS E ARQUITETURA DA SOLUÇÃO

A arquitetura da solução deverá cumprir as seguintes premissas:

1. Todos os equipamentos que integram a solução de rede Wi-Fi proposta pelo concorrente devem ser do mesmo fabricante;
2. Toda a solução deverá ser em formato de appliances físicas (Tipo 1) ou virtuais (Tipo 2), sendo que no caso de serem virtuais, o software deverá funcionar sobre os hypervisors VMWare e/ou HyperV. Em ambas as abordagens, é obrigatório que a arquitetura de alta disponibilidade atenda aos seguintes requisitos:
    a. Redundância local: Funcionamento em cluster totalmente redundante no modo ativo-ativo ou ativo-passivo;
    b. Redundância geográfica: Funcionamento dos clusters numa configuração mínima de 2+1, entre dois centros de dados geograficamente distantes, em modo ativo-ativo ou ativo-passivo. O terceiro cluster, deverá garantir os mecanismos de fail-over e resiliência da solução.
3. No caso de escolha de appliances físicas, o adjudicatário deverá fornecer todos os ativos necessários para garantir o funcionamento completo e contínuo da solução, incluindo todas as plataformas de gestão e serviços respetivos associados;
4. A solução a apresentar deverá ter uma gestão centralizada;
5. Todas as plataformas de gestão e sistemas associados ao normal funcionamento e operacionalização da solução de rede Wi-Fi, deverão ser dimensionadas consoante o tipo de appliances propostas pelo adjudicatário, as quais deverão cumprir com os requisitos mínimos da secção IIÍ.III;
6. Entende-se por "sistemas associados", toda e qualquer plataforma ou serviço adicional, seja esta, no formato de appliances físicas ou virtuais, que complemente a solução de rede Wi-Fi e assegure o desempenho e funcionalidades exigidas. Isso inclui, mas não se limita a, componentes axilares ao controlo de acesso à rede (NAC) e plataformas de configuração centralizada, como soluções baseadas em inteligência artificial (AIOps) para diagnóstico baseado em ferramentas de telemetria;
7. A solução deverá ser implementada exclusivamente em ambiente de alojamento proprietário, não sendo aceitáveis arquiteturas em cloud pública;
8. Deverá ser apresentado um documento com a arquitetura física a lógica de alta disponibilidade proposto pelo ADJUDICATÁRIO.

3.2. MAPA DE QUANTIDADES POR OPÇÃO

Mapa de Quantidades

Descrição	Quantidade
Appliance física – Tipo 1 para solução Wi-Fi. Inclui controladoras wireless com chassi, duas fontes de alimentação (AC), kit de montagem em rack de quatro postes (por nó).	>= 3 Clusters de 3 nós (total 9 nós)
Módulos 40GE QSFP+, da marca do fabricante e compatíveis com padrões de curto alcance (short-reach) e com a norma IEEE 802.3ba. Alcance mínimo de 100m OM4 MMF, 150m over OM4 MMF, de encaixe do tipo LC)	36
SFP 10G SR original do Fabricante (SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant)	36
Cabo em fibra ótica multimodo 50/125 LC/LC OM4 com 1.5 metros	18
Cabo em fibra ótica multimodo 50/125 LC/LC OM4 com 2 metros	18
Cabo em fibra ótica multimodo 50/125 LC/LC OM4 com 3 metros	18
Appliance física – Tipo 1 para solução Wi-Fi NAC e sistemas associados. Inclui: Licenciamento em HA com subscrição por 60 meses:	>= 3 Clusters de 2 nós (total 6 nós)
Plataforma de gestão centralizada das controladoras e APs	
Recursos de segurança e NAC (Network Access Control)	
Visibilidade avançada da rede, incluindo monitorização de desempenho, diagnósticos proativos e otimização baseada em inteligência artificial (AIOps) com recursos a ferramentas de telemetria	
Plataforma de monitorização alarmística e estatística dos APs	
Utilização de todas as funcionalidades avançadas que cumpra no mínimo as especificações do Wi-Fi 6 (dando preferência a tecnologias mais recentes, desde que certificadas pela WI-FI Alliance), como OFDMA, MU-MIMO, entre outros	
Gestão e retenção de registos (logs)	
Appliance virtual – Tipo 2 para solução Wi-Fi. Inclui software para controladoras wireless	>= 9 instâncias
Appliance virtual – Tipo 2 para solução Wi-Fi com NAC e sistemas associados. Inclui: Licenciamento em HA com subscrição por 60 meses:	>= 9 instâncias
Plataforma de gestão centralizada das controladoras e APs	
Recursos de segurança e NAC (Network Access Control)	

Visibilidade avançada da rede, incluindo monitorização de desempenho, diagnósticos proativos e otimização baseada em inteligência artificial (AIOps) com recursos a ferramentas de telemetria	>= 9 instâncias
Plataforma de monitorização alarmística e estatística dos APs	
Utilização de todas as funcionalidades avançadas de Wi-Fi 6 ou superior, como OFDMA, MU-MIMO, entre outros	
Gestão e retenção de registos (logs)	
Instalação e substituição de AP's em produção; **Criar infraestrutura para implementar 6500 novos acessos para AP's** **Inclui todos os acessórios necessários à integração dos AP's;**	**Substituição de cerca de 3500 AP's e instalação de 6500 AP's**
Execução de site surveys. Inclui o estudo e avaliação da cobertura da rede Wi-Fi, com a elaboração de plantas de localização dos pontos de acesso, devidamente integradas na solução proposta	**Entre 1800 e 2000 sites**
Elaboração de um levantamento de necessidades para renovação da infraestrutura passiva identificando todos os materiais apresentadas na Tabela IV.	

3.3. CARACTERISTICAS TÉCNICAS

I. Pontos de acesso Wireless (AP's)	
Requisitos de conformidade com normas e Certificações de Segurança	• O fabricante do equipamento deve assegurar a conformidade com as deliberações da Comissão de Avaliação de Segurança (GNS) e atender às certificações exigidas. Além disso, deve seguir rigorosamente as normas e práticas estabelecidas por entidades reconhecidas, como Wi-Fi Alliance, ETSI, ENISA e NIST. A certificação FIPS é obrigatória para garantir que o equipamento esteja em conformidade com as melhores práticas e regulamentos de segurança da informação

Requisitos Mínimos Por Equipamento (Tipo 1 e 2)

Característica base	
• Sistema de rádio de acordo com a legislação da União Europeia e Portuguesa	2.4, 5 e 6Ghz
• Suporte de Wi-Fi 6E (6Ghz) ou superior	802.11ax ou 802.11be
• Suporte de PoE (802.2at) - sem limitação de funcionalidades	24.4W
• Canais de frequência	20, 40, 80, 160 MHz
• Suporte de mecanismos de criptografia Wireless	WPA2 e WPA3
• Suporte de 802.1x	EAP-TLS, EAP-TTLS, e EAP-PEAP
• Tecnologia de segurança e prevenção de sistemas	wIPS
• Número de SSID	>= 8
• Número de utilizadores simultâneos	>=100
• Acesso via consola	Interface dedicada ou RJ-45
• Duas portas gigabit ethernet com possibilidade de configurar LACP e/ou porta Multi-gigabit (802.3bz);	2x 10/100/1000G 1x 100M/1000M/2.5G
• Suporte metálico	Teto/parede
• MTBF	>=87 600 horas

Características de transmissão	
• Suporte de protocolos wireless	802.11e, 802.11i, 802.11k, 802.11r,802.11w
• Cumprir com 802.11ax, nas frequências 2.4, 5 e 6Ghz, conforme as especificações da norma	>= 4x4 downlink MU-MIMO e OFDMA uplink/downlink.
• Cumprir com 802.11ac, na frequência 5Ghz, conforme as especificações da norma	>= 4x4 downlink MU-MIMO
• Cumprir com 802.11ax, nas frequências 2.4, 5 e 6Ghz, conforme as especificações da norma	>= 4x4 MIMO
• Tecnologias para integração de dispositivos de IoT e eficiência operacional	BLE5 e/ou Zigbee (IEEE 802.15.4)

Configuração e aprovisionamento
• Possibilidade para o aprovisionamento automático dos AP's com recurso a tecnologias de Zero Touch Provisioning.(ZTP)
• Os AP's deverão disponibilizar o firmware próprio para suportar o funcionamento através das controladoras
• Suportar configuração automática baseada em políticas
• Permitir atualizações de software remotamente
• Sistema de indicadores coloridos ou equivalente para diagnosticar estado do AP

Funcionalidades
• Tecnologia "Smart AP", providenciando a diminuição de consumo de energia mediante a utilização das antenas
• Configuração de Preshared key
• MAC blacklist e/ou whitelist
• Suporte de TWT para aumentar o tempo de suspensão em modo inoperacional

• Otimização de sinal com direcionamento de frequência automático • Permitir transmissões simultâneas (BSS coloring) • Combinação de proporção máxima para melhor desempenho do receptor (MRC) • Suporte de funcionalidades contra interferência e falhas de cobertura de sinal (CDD/CSD) • Suporte de tecnologia STBC, para melhorar o alcance e a qualidade de sinal • Capacidade de garantir mecanismos LDPC, para alta eficiência na correção de erros • Garantir a alta disponibilidade das redes serviço em caso de indisponibilidade da controladora
Alta Disponibilidade
• Garantir serviços de rede e autenticação de clientes em modo de funcionamento local • O AP deverá suportar o funcionamento em modo centralizado e local (bridge-mode), dependendo sempre da comunicação/indisponibilidade com a controladora • Deve permitir que o tráfego local possa comunicar diretamente no ponto de acesso (routing-local), sem necessidade de redirecionar o tráfego para o controlador central

II. Cluster de Controladoras e Sistemas Associados

Requisitos de conformidade com normas e Certificações de Segurança	• O fabricante do equipamento deve assegurar a conformidade com as deliberações da Comissão de Avaliação de Segurança (GNS) e atender às certificações exigidas. Além disso, deve seguir rigorosamente as normas e práticas estabelecidas por entidades reconhecidas, como Wi-Fi Alliance, ETSI, ENISA e NIST. A certificação FIPS é obrigatória para garantir que o equipamento esteja em conformidade com as melhores práticas e regulamentos de segurança da informação

Requisitos Mínimos Por nó de Cluster (Tipo 1 e 2)

Característica base (Tipo-1)	
• Número de portas Gigabit SFP+ 10 Gbit/s	>= 4
• Número de portas Gigabit QSFP+ 40 Gbit/s	>= 2
• Porta de gestão dedicada "Out of Band"	Sim
• Número de portas de alta disponibilidade 1Gbit/s	>= 1
• Número de portas de alta disponibilidade 10 Gbit/s SFP+	>= 1
• Porta USB	>= 1
• Porta de consola	Obrigatório
• Disco rígido SSD	>= 16GB
• Throughput mínimo	>= 40 Gbps
Característica base	
• Número de clientes por cluster	>= 120 000
• Número de AP's por cluster	>= 30 000
• Suporte de SNMP com MIB públicas	SNMPv2 e v3
• Suporte de endereçamento IP	IPv4 e IPv6
• Protocolo LLDP	802.1AB
• Número de VLAN's	>= 4000
• Número de redes wireless	>= 4000
• Possibilidade de configurar redes/SSID em cada AP na mesma frequência, com métodos de autenticação dos clientes independentes e distintos	>= 8 SSID
• Pelo menos 8 redes/SSID terão de suportar encriptação da comunicação	WPA3
• Garantir mecanismos de segurança no acesso ao captive portal	>= TLS 1.2 e HTTPS
• Tráfego de cliente deverá ser encriptado por cada SSID	IPSec DTLS, entre outros
• Capacidade de atualizar o firmware/software de todos os AP centralmente	Obrigatório
• Certificação Wi-Fi Alliance	802.11a/b/g/n/ac/ax ou be
• MTBF	>=87 600 horas

• Acondicionamento do hardware	Rack de 19"
Desempenho	
• Número ativo de sessões	>= 1 Milhão
• Número de sessões IPsec simultâneas	>= 30 000
• Suporte de throughput mínimo por IPSec	>= 20 Gbps

Gestão centralizada e Arquitetura
• Gestão e administração da própria appliance através de interface web, linha de comandos e API XML
• Suporte de mecanismos de automação de configurações sobre SSH (ex: NETCONF, RFC 6241, 6242)
• Suporte de linguagem de modelação de dados (ex: YAN, RFC 6020)
• Na gestão centralizada deve existir a possibilidade de criar diferentes perfis de utilizadores para administração para a gestão da appliance, com diferentes níveis de privilégio
• Possibilidade de editar configurações pendentes que ainda não foram aplicadas
• Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas
• Possibilidade de descartar alterações à configuração realizadas
• Possibilidade de armazenar diferentes versões da configuração
• Na gestão centralizada deve existir a capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada
• Na gestão centralizada deve existir um ponto centralizado para efetuar upgrades e atualizações de versões
• Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de AP's
• Na gestão centralizada deve ser possível gerir todas as controladoras
• Os AP terão de ser controlados de forma centralizada
• O número de clientes mínimo proposto, não poderá estar limitado ao número de registos de utilizadores ou AP's ao longo do tempo de vida da solução;
• Cada SSID deverá possibilitar o mapeamento de uma VLAN de serviço sobre as redes de aprovisionamento da solução
• O tráfego dos clientes poderá ser encaminhado através um túnel encriptado por SSID até a um ponto central onde depois será encaminhado para a internet ou para outras redes (aplicação de regras de routing e filtragem de acessos em layer 4)
• O tráfego entre redes (SSID) terá de estar isolado entre si e do restante tráfego infraestrutura, em todos os troços existentes entre o AP e um ponto local ou central (controlador)
• Suporte de roaming entre AP sem necessidade de autenticação
• O funcionamento das redes terá de ter a opção de ser disponibilizado de forma automática, apenas num intervalo de tempo pré-definido (ex: durante horário de funcionamento de cada local) por SSID
• Possibilidade de habilitar e/ou desabilitar protocolos (ex. 802.11b) por SSID
• Definição de número máximo de utilizadores por ponto de acesso/SSID
• Prioridade da rede/SSID relativamente aos restantes
• Limitação da largura de banda por utilizador ou grupo de utilizadores e/por rede em cada local e/por aplicação
• Roaming automático de utilizadores entre AP e frequências
• Gestão automática dos canais a utilizar pelos AP, otimizando o uso do espectro rádio e minimizando a interferência
• Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento
• Possibilidade de envio seletivo de logs, de acordo com o nível de severidade
• Serviços/Servidor de DHCP, NTP e DNS incluído

Energia e Alimentação (Tipo 1)	
• Alimentação AC	100–240V AC, 50–60 Hz
• Consumo de energia médio	<= 520 W
• Consumo de energia máximo	<= 600 W
• Dissipação Térmica	<= 2100 BTU/h
• Fonte de alimentação redundante hot-swappable	SIM
Condições ambientais (Tipo 1)	
• Temperatura de funcionamento	0 - 40 °C
• Humidade	5 a 90% sem condensação
• Compliance	FCC Part 15 Class, VCCI, UL, CAN/CSA-C22.2 No. 60950-1
• Nível de potência sonora	<= 73 (dBA)

Dimensões (Tipo 1)	
• Altura	<= 88.4 mm (2RU)
• Largura	<= 450 mm
• Profundidade	<= 560 mm
• Peso	<= 15 KG

Firewall

- Suporte para diferentes tipos de protocolos: SCTP, TCP, UDP, ICMP, IP
- Visualização de políticas de forma global ou por pares de interface
- Suporte de NAT e PAT
- Configuração de NAT por política
- Traffic shaping e QOS: shaping de tráfego partilhado por política, shapping por IP, largura de banda máxima e garantida, número máximo de ligações por IP, priorização de tráfego

Networking

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: Layer 2, Layer 3
- Suporte de IEEE 802.1AX
- Suporte de protocolos dinâmicos de routing
- Suportar protocolo de balanceamento de pacotes em layer-3: ECMP (RFC 2992)
- Garantir mecanismos de redundância de equipamentos através de IP: VRRP (RFC 2338, RFC 5798)
- Suporte de routing estático
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas

Segurança

- Filtragem de conteúdos web por categorias pré-definidas, com a possibilidade de configuração de whitelists e blacklists manuais
- Controlo de aplicações por categorias pré-definidas
- Controlo de acessos a botnet baseadas em listas dinâmicas (subscrição associada ao suporte da solução, com o mesmo período temporal)
- Possibilidade de controlo de acessos a serviços/domínios com base em listas dinâmicas de avaliação da reputação
- Técnicas de prevenção de intrusões (vertente web (acesso dos clientes) e infraestrutura Wi-Fi (wIPS)) com atualizações de assinaturas;
- Identificação e controlo de rogue APs/equipamentos
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas
- As políticas de segurança devem poder ser geridas de forma centralizada
- Possibilidade de criação de zonas lógicas para segregação de tráfego consoante diferentes níveis de segurança

Registo de eventos e Relatórios

- A solução deverá disponibilizar relatórios, a ser gerados numa plataforma central
- Apresentação de número de Utilizadores/Dispositivos/SSID por local em cada momento
- Disponibilização de número de Utilizadores/Dispositivos/SSID por local num determinado intervalo de tempo
- Demonstração de tráfego consumido por Interface WAN/LAN, por AP ou grupo de AP's
- Apresentar as páginas visitadas por categorias
- Desencadear alertas consoante o nível de severidade, eventos específicos, por tipo de ações e destinos com opção para registo parcial ou completo de eventos
- Possibilidade de exportar relatórios em formato Excel e/ou PDF
- Encriptação de eventos para confidencialidade e integridade apenas para utilização de plataformas externas à solução (ex. SIEM)
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a largo prazo (backups)
- Possibilidade de notificar por email o envio de eventos syslog, com a respetiva descrição
- Mecanismo nativo de visualização de eventos de forma estatística, com ferramentas de procura detalhada, disponível através de recurso com web browser
- Registos detalhados de tráfego: tráfego enviado, bloqueado, sessões violadas, tráfego local, pacotes inválidos
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance, de forma que, a partir dos logs criados se possa obter informações de alto nível.

Plataforma de Inteligência artificial

- Deverá ser disponibilizada uma plataforma assente em tecnologia de inteligência artificial (AIOps), que permita à entidade publica contratante, diagnosticar em termos da solução de Wi-Fi:
  - Autenticação:
    i. Tempo excessivo de autenticação e/ou onboarding;
    ii. Falhas de associação e autenticação (várias tentativas, falhas, etc.).
  - Alterações de performance da rede:
    i. Análise do throughput
    ii. Roaming excessivo ou lento
    iii. Frequência utilizadas pelos clientes
    iv. Interferências excessivas
    v. Falhas de cobertura Wi-Fi
    vi. Capacidade de clientes por AP
  - Análise analítica do estado da rede com recurso a baseline da rede (serviços, aplicações, tipo de utilização dos utilizadores), e alerta sobre desvios potencialmente associados a problemas
  - Monitorização do hardware:
    i. Disponibilidade
    ii. CPU, memória
    iii. Crashs
  - Gestão pró-ativa (Indicação da origem do problema e da sua mitigação para a maioria dos eventos)
  - Serviços de integração com o ITSM existente na entidade pública contratante

Alta Disponibilidade

- Permitir a criação de clusters redundante e com suporte a arquiteturas em alta disponibilidade
- Suportar os modos de operação:
  - Ativo-passivo
  - Ativo-ativo
  - Virtual Cluster (apenas para opção-2)
- A solução deverá operar localmente com o mínimo 3 nós por cluster, sendo que, pelo menos 2 nós, deverão ser capazes de suportar o número total de Access Points e utilizadores especificados
- Garantir o failover e recuperação automática de serviço com base em:
  - Monitorização de portas e links
  - Failover local em menos de 1 segundo
  - Notificação automática de eventos de failover
  - Sincronização de sessões
- Suportar a execução de atualizações sem impacto no serviço, garantindo failover automático durante esses procedimentos

III. Componente de Controlo de Acesso à Rede (NAC)

Requisitos de conformidade com normas e Certificações de Segurança	• O fabricante do equipamento deve assegurar a conformidade com as deliberações da Comissão de Avaliação de Segurança (GNS) e atender às certificações exigidas. Além disso, deve seguir rigorosamente as normas e práticas estabelecidas por entidades reconhecidas, como Wi-Fi Alliance, ETSI, ENISA e NIST. A certificação FIPS é obrigatória para garantir que o equipamento esteja em conformidade com as melhores práticas e regulamentos de segurança da informação

Requisitos Mínimos (Tipo 1 e 2)

Característica base	
• Interfaces 10/100/1000 (cobre, RJ-45)	>= 2
• Processador	>= 2 GHz CPU, 16 cores, 32 threads
• Disco SATA SSD	>= 3x 960GB
• Memória (RAM)	>= 128GB
• Número de portas Gigabit 10 Gbit/s (SFP+)	>=4
• USB Ports 3.0	>= 2
• Porta de série (conetor RJ45)	RS-232
• Suportar níveis de RAID	5 e/ou 10
• Licenciamento sem restrição temporal para utilizadores simultâneos	120 000
• Acesso de administração via HTTPS	TLS1.2 e/ou 1.3
• Suporte SNMP com MIB públicas	SNMPv2 e v3
• Suporte de endereçamento IP (sistema e clientes)	IPv4 e IPv6
• Suporte de autenticação de AP's e switchs	802.1x
• Montagem em Rack 19”	<= 2U

Funcionalidades e Arquitetura

- O NAC deverá obrigatoriamente integrar com a solução apresentada para os acessos Wi-Fi
- Esta componente deverá funcionar em cluster totalmente redundante no modo ativo-ativo ou ativo-passivo local e entre dois centros de dados geograficamente distantes, numa configuração mínima de 2+1;
- Possibilidade de exportar os registos por syslog para integração com sistemas externos (ex. SIEM);
- A solução deve ser capaz de garantir a segurança dos acessos aos recursos internos como também às aplicações de cloud
- A plataforma deve permitir:
  - Templates de implementação para qualquer rede
  - Autenticação por MAC, suporte de captive portal e 802.1x
  - Relatórios, suporte de analítica e ferramentas de despiste de problemas
  - Suporte de registo de múltiplos equipamentos (convidado, BYOD, e equipamentos não geridos) com indicação da data e hora de acesso
- Verificação de estado dos terminais (posture validation):
  - Windows 10 ou superior:
    i. Patchs do sistema operativo
    ii. Antivírus
    iii. Verificação de serviço
    iv. Verificação de aplicação instalada
    v. Verificação de ficheiro
    vi. Entradas no registry (chave, valor, etc.)
  - MacOS:
    i. Antivírus
    ii. Verificação de serviço
    iii. Verificação de ficheiro
    iv. Verificação de aplicação instalada

v. Gestão de patch

- A solução tem de suportar múltiplos mecanismos de controlo de acessos (802.1x, listas de acesso, atribuição de VLAN, redireccionamentos de URL, entre outros)
- A solução tem de garantir o acesso à infraestrutura numa VLAN isolada enquanto o PC e/ou o utilizador não providenciarem credenciais válidas e/ou atualizarem a postura do sistema
- Suporte de integração com o UEM/MDM/MAM Microsoft Intune® e com pelo menos 2 das seguintes soluções:
  - VMWare AirWatch®
  - IBM MaaS360®
  - Ivanti Mobile Iron®
  - Citrix Endpoint Management®

Autenticação

- A solução a apresentar deverá garantir o suporte dos seguintes tipos de acesso:
  - Wired (switchs)
  - Wireless (Wi-Fi)
  - VPN
- Suporte dos seguintes tipos de autenticação:
  - 802.1X
  - RADIUS
  - SAML v2.0 ou OAuth2.0 ou OpenID
  - LDAPS
  - EAP-TTLS
  - EAP-TLS
  - Captive Portal para as redes Wi-Fi de visitantes com as seguintes funcionalidades:
    i. Aceitação de termos de responsabilidade
    ii. Possibilidade de registo de utilizador e receção de token via SMS
    iii. Possibilidade de registo de utilizador e receção de token via email
    iv. Possibilidade de registo e validação simples de email
    v. Possibilidade de definir captive portais com conteúdos distintos por local
    vi. Definição de landing page após autenticação com sucesso;
    vii. Acesso patrocinado (auto-login com autorização por elemento interno)
    viii. Autenticação via redes sociais (pelo menos 3 das seguintes):
      a. Facebook
      b. Google
      c. LinkedIn
      d. Twitter
      e. Instagram

Energia e Alimentação (Tipo 1)	
• Alimentação AC	100–240V AC, 50–60 Hz
• Consumo de energia médio	<= 1400 W
• Consumo de energia máximo	<= 1600 W
• Dissipação Térmica	<= 2100 BTU/h
• Fonte de alimentação redundante hot-swappable	SIM

Condições ambientais (Tipo 1)	
• Temperatura de funcionamento	5 - 40 °C
• Humidade	5 a 90% sem condensação
• Compliance	FCC Part 15 Class, VCCI, UL, CAN/CSA-C22.2 No. 60950-1
• Nível de potência sonora	<= 73 (dBA)

Dimensões (Tipo 1)	
• Altura	<= 88.4 mm (2RU)
• Largura	<= 450 mm
• Profundidade	<= 560 mm
• Peso	<= 20 KG

IV. Levantamento de Requisitos

Requisitos de conformidade com normas e Certificações de ITED e Telecomunicações	• O adjudicatário deve garantir que o levantamento das necessidades da rede passiva, incluindo o site survey e a análise dos sistemas de backbone, para garantir o suporte da nova solução, de acordo com as normas ISO e regulamentos de telecomunicações. Este levantamento deve ser realizado por profissionais certificados em ITED ou telecomunicações, assegurando a precisão e o sigilo dos dados obtidos. O processo deve atender rigorosamente aos requisitos das normas descritas.

Requisitos Mínimos Por Site

Site Suvey	
• Preparação do site survey	Levantamento de Infraestrutura, Localização dos APs atuais, elaboração de plantas do local
• Testes de cobertura e potência de Sinal	Testes de cobertura globais Medição de potência e receção de sinal, identificar áreas a melhorar
• Teste de relação sinal-ruído (SNR)	Medir o impacto de interferências e barreiras físicas
• Análise da frequência do canal de operação	Estudo da ocupação dos canais e sobreposição de frequência
• Testes de desempenho da conectividade em modo VHT	Analisar a taxa de transferência e estabilidade
• Testes de sinal com base nas normas	802.11a/b/g/n/ac/ax/be
• Testes de performance em diferentes canais	20/40/80/160/320MHz
• Análise de interferências externas	Micro-ondas, eletromagnetismo, radiofrequência, elevadores, iluminação, etc
• Integração das plantas de localização dos novos APs	Formato compatível com a solução Wi-Fi
• Prazo para a entrega do site survey	Até 60 dias após o início do projeto

Infraestrutura Passiva	
Necessidades	**Identificação**
• Identificação de toda a infraestrutura passiva em operação	Tomadas RJ45, cabos UTP, fibras multimodo/monomodo, painéis de ligação e todos os acessórios
• Levantamento e planeamento da renovação dos subsistemas	Substituição e modernização de subsistemas horizontais e verticais (piso e edifício)
• Análise de capacidade, expansão e escalabilidade da rede	Avaliar lotação de bastidores, alocação de interfaces de equipamentos ativos, número de cabos entre bastidores
• Garantir que os materiais estão em conformidade normativa	Cabos de cobre Cat-6A (TIA/EIA-568-C.2), fibras OM3 (50/125µm) com conectores e acessórios compatíveis
• Quantificação de tomadas de rede com encaixe RJ45	Substituição de tomadas RJ45 inferiores ao padrão Cat-6A por novas tomadas Cat-7
• Determinação do número de painéis de ligação de cobre blindado e a sua categoria	Painéis compatíveis com cabos com suporte a encaixe RJ45, de 1U para montagem em Rack 19"

• Quantificação de patch cords em cobre blindado e respetivas medidas	Patch cords e respetiva categoria com conectores RJ45 cravados
• Quantificação de fibra ótica (monomodo e/ou multimodo) entre painéis de ligação	Tipo de fibras óticas e identificação de conetores
• Determinação número de painéis de ligação de fibra ótica	Painéis compatíveis com fibras óticas com suporte a encaixes a identificar, de 1U em Rack 19"
• Testes de certificação nos componentes passivos propostos a manter	Testes de atenuação e desempenho nas fibras óticas e/ou cabos de categoria 6A ou superior
• Elaboração de um mapa de quantidades geral (total) e específico (por site)	Qualificar e quantificar todo o material necessário à restruturação e certificação da rede passiva
• Planeamento de logística com cronograma	Segmentar todo o material para entrega nas entidades
• Prazo de entrega do levantamento de requisitos	Até 60 dias após o início do projeto

3.4. SERVIÇOS DE INSTALAÇÃO E SUPORTE

SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO A INCLUIR NA OPÇÃO DE AP's e APPLIANCES PROPOSTAS (TIPO 1 e 2)		
Fase 1	a) Serviço de Instalação e Configuração de Clusters de Appliances: Inclui a montagem (apenas para Tipo-1) e a configuração de clusters de appliances na infraestrutura existente nos centros de processamento de dados ou áreas técnicas a definir pelo adjudicante.	Chave-na-mão
Fase 2	a) Serviço de Instalação e Configuração de Pontos de Acesso Wireless: Inclui a montagem e a configuração dos pontos de acesso sem fios, tanto nas infraestruturas passivas a serem implementadas quanto nas existentes, bem como nos equipamentos ativos das entidades. O serviço também abrange a realização de um site survey para validar e comprovar a localização dos APs definida no levantamento de requisitos. Este processo inclui a adição das plantas de localização e dos equipamentos com a execução de testes de sinal para assegurar a cobertura e o desempenho proposto.	Chave-na-mão
	b) Serviço de levantamento da Rede Passiva: Inclui a análise completa da rede passiva existente, conforme detalhado no levantamento de requisitos. Este serviço abrange a identificação de todas as infraestruturas passivas necessárias à reformulação da rede para Cat-7, incluindo tomadas RJ45, cabos UTP, fibras multimodo e monomodo, painéis de ligação, bastidores e acessórios intrínsecos à renovação dos subsistemas de área de trabalho, horizontais (piso) e de edifício.	Chave-na-mão

Serviço de operacionalização on site para aplicações críticas (incluindo manutenção de todo o software proposto) para 36 Meses 24x7	
• Nível de Serviço	24x7
• Tempo de resposta	4 horas
• Tempo de resposta para incidentes críticos	30 minutos
• Solução de suporte que permita a abertura automática de chamadas, no caso de incidentes de falha ou pré-falha de algum componente de hardware	Sim
• Os serviços de reparação deverão ser realizados apenas por técnicos de equipas residentes em Portugal e devidamente credenciados pelo fabricante do equipamento	Sim

• A reparação de Hardware deverá apenas ser realizada com peças genuínas do fabricante dos equipamentos	Sim
• Deverá ser disponibilizado um portal/ferramenta que permita uma visão global e em tempo real do estado de suporte de todos os equipamentos registados. Deverá também permitir a abertura de chamadas de suporte e o acompanhamento de todos os casos abertos	Sim
• Suporte disponibilizado sempre em português durante todo o horário de cobertura (24x7) e através de um único ponto de contacto para todo o tipo de incidentes de Hardware	Sim
• Deverá ser atribuído um responsável pela coordenação e planeamento das atividades de suporte preventivo e que, semanalmente, esteja presente em reuniões presenciais para apoio às ações proativas a serem executadas e a revisão de ações que estejam planeadas	Sim
• Declaração do fabricante onde conste o conhecimento técnico da infraestrutura e responsabilidade pela solução apresentada na proposta	Sim

Serviços Profissionais de Fabricante:
Toda a solução terá de estar coberta com garantia/suporte de fabricante A garantia/suporte tem de incluir: - Suporte remoto de fabricante 24x7 - Suporte a diagnóstico e acesso a todos os softwares updates - Acesso a portal de suporte do fabricante - Substituição avançada de hardware (inclui Chassi – caso se aplique, power supplies, módulos, fans e transceivers) - Capacidade de abertura de casos diretamente no fabricante, sem ter de recorrer a qual processo que envolva terceiras partes - Duração mínima de 3 anos (com data de início de garantia/suporte a coincidir com a data de início de projeto) - Serviços de consultoria de Fabricante

3.5. PLANEAMENTO E IMPLEMENTAÇÃO

1. **Nos valores a apresentar, devem estar previstos os seguintes trabalhos de pré-instalação e implementação da solução Wi-Fi:**
   a) Plano de projeto detalhado, incluindo metodologia de gestão de projeto, plano de trabalhos, mecanismos de acompanhamento e entregáveis de projeto, tendo em consideração os elementos a entregar pelo ADJUDICATÁRIO;
   b) O projeto de implementação correspondente à Fase 1 e à Fase 2 da alínea a), deverá ter os seguintes milestones:
      i. Atribuição de um gestor de projeto dedicado;
      ii. Elaboração e desenvolvimento da arquitetura técnica e funcional a implementar, com recomendações de melhorias e melhores práticas;
      iii. Planeamento de execução de tarefas para implementação da solução;

iv. Elaboração do High Level Design e Low Level Design;
v. Planeamento de tarefas para testes de aceitação e validação da solução implementada;
vi. Nos sites deverão ser substituídos todos os AP's e respetivos suportes (é obrigatório o fornecimento do material necessário operacionalidade do equipamento);
vii. Nos centros de processamento de dados da SPMS, a instalação física dos equipamentos será em rack (é obrigatório o fornecimento de todo o material por forma a garantir a instalação física dos equipamentos e sua interligação à estrutura de switching);
viii. Updates e upgrades para versões de software recomendadas;
ix. Testes de failover (redundância física e lógica);
x. Configuração dos novos equipamentos de acordo com o planeado em sede de projeto;
xi. Migração dos serviços para os novos equipamentos (devido à criticidade das aplicações, deverá ser feito em várias fases para diminuir probabilidade de riscos associados à migração);
xii. Testes de aceitação em cada uma das fases da migração;
xiii. Acompanhamento da solução implementada por, pelo menos, 12 meses após o fecho do projeto;
xiv. Todos os trabalhos de planeamento, instalação, configuração, migração e testes têm de ser realizados on-site;
xv. Entrega de documentação do projeto, passagem de conhecimento, e formação certificada pelo fabricante a 15 elementos da equipa da SPMS;
xvi. Dossier com o cadastro de rede;
xvii. Relatório com todas as parametrizações da solução, nomeadamente desenhos técnicos detalhados da arquitetura em operação, acompanhados a documentação da memória descritiva que descreva as configurações na vertente física e lógica.

c) Execução do projeto de levantamento de requisitos referente à Fase 2 da alínea b) deverá abranger a identificação quantitativa e qualitativa das necessidades, estruturada nas seguintes fases:
i. Atribuição de um gestor de projeto
ii. Realização de um site survey em cada local do Ministério da Saúde;

iii. Testes de cobertura, teste de potência de sinal de receção, testes de relação sinal-ruído (SNR), frequência do canal de operação;

iv. Testes de conetividade em modo VHT (Very high throughput) e em modo legado;

v. Testes de compatibilidade com as versões anteriores (normas, 802.11/a/b/g/n/ax);

vi. Teste de performance em modo VHT em condições de diferentes modelos de canal.

d) Mediante os resultados da alínea b), deverão ser identificadas as áreas com cobertura insuficiente ou qualidade de sinal inadequada, bem como determinar o número de AP´s em falta;

e) Nos casos em que o Adjudicante não forneça as plantas de arquitetura, deverá ser realizado o levantamento topográfico dos espaços, para elaboração das plantas arquitetónicas a fornecer;

f) Realizar um levantamento completo de toda a componente passiva em produção, identificando detalhadamente todos os materiais implementados. O ADJUDICATÁRIO deverá apresentar um mapa de quantidades que especifique os materiais existentes.

g) Elaborar um planeamento de reestruturação do subsistema de backbone horizontal dos locais, incluindo a passagem dos cabos UTP, desde as tomadas de rede até os distribuidores de piso;

h) Na componente passiva é obrigatório quantificar (mapa de quantidades) todo o material imprescindível, como as tomadas do tipo RJ45 (Cat-7), cabos UTP (Cat-7) com e sem ficha RJ45, painéis de ligação e todos os acessórios necessários à interligação dos AP's com os equipamentos ativos;

i) Compilação e entrega de documentação com toda a informação obtida, incluindo o levantamento das necessidades, mapa de quantidades, resultados do site survey com especificações técnicas detalhadas e a localização proposta dos APs;

j) Desenvolver um plano de mitigação de riscos que identifique possíveis desafios ou constrangimentos que possam surgir durante a futura fase de instalação;

k) Considerar a logística e cronograma de entrega dos materiais e/ou equipamentos necessários para a implementação futura.

l) Todas as tarefas que impliquem paragem de serviços ou indisponibilidade de recursos IT críticos da SPMS devem ser obrigatoriamente contempladas fora do horário normal de trabalho, ou seja, após as 20h

2. **Nos valores a apresentar, deve estar prevista garantia nos seguintes termos:**
    a) Prazo de mínimo de 3 (três) anos a contar da data de entrega dos equipamentos, com direito a atualizações do sistema operativo sem encargos adicionais.
    b) Durante o período referido no número anterior, o adjudicatário deverá garantir os serviços e acompanhamento da solução, designadamente:
        a) da solução Wi-Fi;
        b) da solução NAC.
    c) A Entidade Publica Contratante aceitará para os efeitos uma solução que apresente software Perpétuo.

IV. FORMA DA CONSULTA

É imperativo que a consulta preliminar ao mercado seja conduzida com transparência e não haja tratamento desigual de operadores económicos, conforme dispõe o artigo 35.º-A do Código dos Contratos Públicos.

Assim, a consulta preliminar ao mercado será publicitada no portal de internet público da SPMS, EPE, em http://www.spms.min-saude.pt, e no respetivo *LinkedIn*, devendo os operadores económicos interessados em apresentar contributos no âmbito da presente Consulta Preliminar, remeter email para consulta.preliminar@spms.min-saude.pt, até ao dia **28 de outubro de 2024**.

V. PRESTAÇÃO DE INFORMAÇÃO PELOS OPERADORES ECONÓMICOS

A prestação voluntária de informação pelos operadores económicos, deverá ser efetuada para o correio eletrónico consulta.preliminar@spms.min-saude.pt até à data-limite de 28 de outubro de 2024, devendo os interessados indicar claramente no assunto do email a referência "Consulta Preliminar – Equipamentos de Wi-Fi".

VI. INFORMAÇÃO PRETENDIDA

A informação a prestar voluntariamente pelos operadores económicos, considerada por eles como oportuna e relevante, é a seguinte:

- Informação do equipamento, serviço ou do seu portefólio, com os detalhes que considerar relevante para o objeto da consulta preliminar.
- Os operadores económicos deverão apresentar o ficheiro Excel em anexo à presente Consulta Preliminar, devidamente preenchido.

VII. PRAZO DA CONSULTA

A informação prestada pelos operadores económicos será aceite até à data de **28/10/2024.**