CONSULTA PRELIMINAR AO MERCADO DAG/DIRS Nº 09/2024

Clusters de Balanceadores de rede

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 e instalação que permitam a ampliação e modernização da capacidade de salvaguarda de dados nos seus centros de processamento de dados, pelo

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61 | 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

que 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 instalação;
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 dos equipamentos;

A consulta preliminar será constituída por:

a) 1 Cluster de balanceadores/Publicadores de Gama Média

b) 1 Cluster de balanceadores/Publicadores de Gama Alta

c) Serviços de Instalação, configuração das plataformas a concurso

d) Serviços de Assistência Técnica Preventiva e Corretiva durante o período de 12 meses com cobertura 24 x 7 com 4h de tempo de resposta para os equipamentos referidos em a) e b)

e) 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) e b)

Quantidades de equipamento a adquirir

i	**Cluster de balanceadores/Publicadores de Gama Média**	1
ii	**Cluster de balanceadores/Publicadores de Gama Alta**	1
iii	**Serviços de Instalação, configuração das plataformas a concurso – valores separados para i e ii**	1
iv	**Serviços de Assistência Técnica Preventiva e Corretiva o período de 12 meses com cobertura 24 x 7 com 4h de tempo de resposta, - valores separados para i e ii**	1

v	**Serviços de Assistência Técnica Preventiva e Corretiva durante o período de 12 meses com cobertura 24 x 7 com 4h de tempo de Resposta, valores separados para i e ii**	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.

Características Técnicas dos Equipamentos

i) Cluster de balanceadores/Publicadores de Gama Média	
Requisitos de Segurança da Autoridade Nacional de Segurança (GNS)	• O fabricante do equipamento deverá cumprir as deliberações da Comissão de Avaliação de Segurança nomeadamente os critérios objetivos de segurança, assim como o seu âmbito técnico de aplicação, que justificam e fundamentam medidas destinadas a garantir um elevado nível comum de segurança da informação na União Europeia

Requisitos Mínimos	
Características base	
• Número de Nós	2
• Balanceamento de carga de Layer 4 e Layer 7	Sim
• Balanceamento de múltiplos protocolos e possibilidade de recurso a diferentes profiles (nomeadamente, HTTP, HTTP/2, SSL/TLS, FTP, DNS, RTSP, ICAP, Radius, SIP, SMTP, entre outros) de modo a controlar o estabelecimento de ligações, persistência de sessões e autenticação de clientes.	Sim
• Balanceamento de tráfego baseado em mútiplos algortimos/métodos estáticos e dinâmicos de balanceamento para aplicação ou servidor, tais como, round robin, least connections, fastest, ratio, observed e predictive.	Sim
• Stickeness de sessões recorrendo a diversos métodos desde mecanismos simples baseados no endereço IP de origem e de destino e SSL persistence a mecanismos avançados, tais como, Microsoft RDP, cookie passive, cookie rewrite, cookie insert. Possibilidade de recorrer a um motor avançado de scripting (TCL-based) totalmente configurável de modo a permitir a persistência de sessões com base na informação disponível no payload de pacotes.	Sim
• Health monitoring aplicacional suportando múltiplas probes aplicacionais pré-construídas incluindo, HTTP/s, SMTP, Radius, SNMP, TCP e outros. Possibilidade de criação/personalização de probes por via de motor de scripting avançado e simplificado.	Sim
• Mecanismos de caching e compressão ao nível da RAM aplicável a objectos com elevado número de pedidos e conteúdos estáticos, tais como, CSS, javascript, imagens ou logos.	Sim
• Offload por hardware de encriptação de SSL/TLS	Sim
• Suporte de algoritmos de encriptação	GCM, ECC, DSA, RSA, Camellia

• Possibilidade de crescimento horizontal da solução	>= 8 equipamentos em cluster
• Gestão dos equipamentos com suporte de autenticação de utilizadores via Radius e LDAP com a capacidade de implementar níveis de acessos distintos por utilizador para operação e visualização, baseados no método RBAC (Role Base Access Control);	Sim
Características de Desempenho	
• Throughput de Layer 4	>=95Gbps
• Throughput de Layer 7	>=60bps
• Bulk encryption	>=35bps
• Hardware Compression	>=35bps
• Hardware DDoS Protection	>=80M SYN Cookies
• Número de requests per second em Layer 7	>=2.5M
• Número de connections per second em Layer 4	>=1M
• Número de requests per second HTTP em Layer igual ou superior a 18M	>=18M
• Número de ligações concorrentes de Layer 4	>=75M
• Número de SSL transactions per second	>=60K (2K SSL TPS)
Características Físicas	
• Interfaces 100G/40G QSFP+/QSFP28	>=2
• Interfaces 25G/10G SFP28/SFP+	>=8
• Porta de gestão dedicada RJ45 (1 Giga);	>=1
• Porta consola Serial dedicada RJ45	>=1
• Interface USB	>=1
• Disco SSD	>= 1TB
• Nº CPUs disponíveis para tenancy	>=12
• GB Memória	>=128GB
• Ocupação em Rack;	Máximo 1U
• Multi-Tenancy	Mínimo 8 tenants
• Fontes de alimentação redundantes certificadas 80 Plus Platinum,	Sim
• LCD com ecrã tátil no painel Frontal	Sim
Certificações de Segurança	
• ANSI/UL 60950-1-2014	Sim
• CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005,	Sim
• A1:2009+A2:2013	Sim
• EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	Sim

• IEC 62368-1:2014 (Second Edition)	Sim
• EN 62368-1:2014+A11:2017	Sim
• CSA C22.2 No. 62368-1-14, UL 62368-1, 2nd Editions	Sim
Standards de Mercado	
FCC Class A (Part 15), IC Class A; VCCI Class A	Sim
• EN 55032:2012/AC:2013 Class A	Sim
• EN 55035:2017	Sim
• EN 300 386 V1.6.1 (2012)	Sim

SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO	
• Serviço de Instalação e Configuração 1 Cluster de balanceadores/Publicadores de Gama Média com instalação na infraestrutura existente.	Chave-na-mão

SERVIÇOS DE ASSISTÊNCIA TÉCNICA PREVENTIVA E CORRETIVA PARA 1 CLUSTER DE BALANCEADORES/PUBLICADORES DE GAMA MÉDIA	
Serviço de operacionalização on site para aplicações críticas (incluindo manutenção de todo o software proposto) para 12 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

ii) Cluster de balanceadores/Publicadores de Gama Alta	
Requisitos de Segurança da Autoridade Nacional de Segurança (GNS)	• O fabricante do equipamento deverá cumprir as deliberações da Comissão de Avaliação de Segurança nomeadamente os critérios objetivos de segurança, assim como o seu âmbito técnico de aplicação, que justificam e fundamentam medidas destinadas a garantir um elevado nível comum de segurança da informação na União Europeia

Requisitos Mínimos	
Chassis, Módulos, e conexão Física	
2 (dois) Chassis Modulares com capacidade de suportar, no mínimo, oito (8) módulos de Data Plane	
2 (dois) módulos de Data Plane com suporte a Balanceamento de Tráfego e WAF	
2 (dois) módulos de Data Plane com suporte a Balanceamento de Tráfego, WAF e DNS	
8 (oito) transceivers 40GBASE SR BIDI	
CARACTERÍSTICAS FÍSICAS E DE DESEMPENHO	
• Para todos os componentes, especificados, o(s) sistema(s) operativo(s) têm de ser, de propósito específico (não de uso geral) e desenvolvido pelo fabricante especificamente para funções de balanceamento de tráfego, aplicações IP (TCP/UDP) e serviços web	Sim
• Plataforma de hardware de modular (chassi), com dimensionamento da capacidade de processamento através da inserção de módulos de Data Plane	Sim
Características mínimas do Chassi modular	
• Ocupação máxima de rack 4U e ajustável a racks de 19"	
• Capacidade de suportar, no mínimo, 8 módulos de Data Plane	
• Possuir, no mínimo, 2 fontes de alimentação AC com opção de expansão para até 4 por chassis.	
• Possuir, no mínimo, 2 controladores de sistema, por chassis	
• Mínimo de 32GB DDR4 de memória RAM	
• Disco Rígido SSD com pelo menos 940 GB	
• Pelo menos uma porta USB 3.0	
• Pelo menos uma porta Serial de Consola	
• CPU com o mínimo de 8 núcleos Intel	

Características de desempenho mínimo para módulos de Data Plane
• Mínimo de 128 GB DDR4 de memória RAM
• Performance mínima de balanceamento L7 >= 90 Gbps
• Número de transações por segundo >= 2 900 000
• Número de conexões por segundo (layer 4) >= 1 100 000
• Capacidade de compressão por hardware >= 62 Gbps
• Processador Intel de 14 núcleos com um mínimo de 28 processadores lógicos
• Disco Rígido SSD com pelo menos 950 GB
Requisitos conectividade para módulos de Data Plane
• Pelo menos 2 (duas) portas QSFP28 com suporte para, no mínimo, às seguintes velocidades: 100 Gbps, 40Gbps, 25Gbps, 10Gbps
• Pelo menos 1 (uma) porta USB 3.0
Requisitos mínimos de gestão de tráfego de SSL por módulo de Data Plane
• Aceleração SSL por hardware (incluindo criptografia ECDSA de hardware)
• Transações por segundo SSL/TLS (ECDSA P-256) >= 70 000
• SSL bulk throughput >= 50 Gbps
• Suporte, no mínimo, a chaves SSL de 1024, 2048 e 4096 bits
• Suporte obrigatório a AES, AES-GCM, SHA1/MD5 e algoritmos de chave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) e Elliptic-Curve Cryptography (ECC)
• Assinatura criptográfica de cookies para verificação de integridade
• Aceleração SSL/TLS híbrida SW/HW (possibilidade de processar SSL simultaneamente no hardware do acelerador e no CPU do sistema)
Requisitos obrigatórios de Virtualização
• Capacidade de virtualização de dispositivos em pelo menos 24 instâncias do sistema operativo em execução simultânea (cada uma com alocação independente de recursos de CPU e memória)
• Cada ambiente virtual pode ser implementado de forma independentemente e com uma versão diferente de firmware e/ou sistema operativo
• Todas as funcionalidades têm obrigatoriamente que estar disponíveis em todas as instâncias virtuais sem a necessidade de licenças adicionais
• Capacidade de compartilhar Vlans entre instâncias de virtualização
Suporte obrigatório aos seguintes padrões de rede
• Padrões de rede suportados: VLAN 802.1q, 802.3ad, NAT, sNAT , IPV6 (incluindo função de gateway entre redes IPv6-IPv4), suporte a domínios de roteamento independentes com capacidade de sobreposição de endereçamento IP.
• Capacidade de criação de túneis IPSEC LAN -to- LAN
• Certificação pelo ICSA Labs como um dispositivo IPSEC 1.3
Suporte obrigatório às seguintes capacidades/features de administração do sistema

• Sistema de administração completamente independente do sistema de processamento de tráfego
• Gestão de dispositivos via CLI (Command Line Interface) via SSH
• Interface gráfica de gestão baseada em HTTPs
• Módulo de gestão (tipo de Lights Out) que permite ligar/desligar o sistema remotamente e visualizar o processo de boot
• Integração, no mínimo, com Active Directory Windows 2003 ou superior, LDAP, RADIUS
• Capacidade de comunicação criptografada com o equipamento e autenticação de administradores/supervisores com certificados digitais
• Suporte para envio de alertas e eventos para um sistema centralizado através de: o Protocolo SysLog e HSL (High Speed Logging) o Notificações via SMTP o SNMP versão.2.0 ou superior
• Interface gráfica com dashboard personalizável que permita monitorizar o estado do equipamento em tempo real
• Módulo de relatórios que permita exibir graficamente o comportamento das aplicações web: latências, throughput para servidores, latências em URLs , endereços IP de origem, URLs mais visitados e outras estatísticas de serviços e servidores balanceados
• Templates para implementação rápida de aplicações conhecidas do mercado (no mínimo Oracle, Microsoft, SAP e IBM) e possibilidade de criação de templates customizados que podem ser atualizados/exportados
• Gestão e monitorização através da API REST permitindo integração tanto imperativa quanto declarativa (configuração de um serviço completo através de uma única chamada REST)
• Automação usando módulos Ansible suportados pelo fabricante
• Possibilidade de sincronização de configuração incremental
Capacidades de funções de balanceamento para módulos de Data Plane:
• Recursos de balanceamento de tráfego para aplicações baseados em TCP/UDP, incluindo serviços da web
• Arquitetura full proxy, com controlo de entrada e saída de conexões, distinguindo conexões do lado do cliente e do lado do servidor
• Possibilidade de definir um endereço IP e uma porta virtual para a prestação de um serviço, associado a uma farm de servidores identificados por um endereço IP e uma porta de serviço igual ou diferente da apresentada ao público
• Capacidades de Balanceamento de tráfego: o Suportar pelo menos os seguintes algoritmos: menos conexões (por membro e por nó), menos sessões, proporção, proporção dinâmica, conexão mais rápida (observada e preditiva) o Balanceamentos personalizados através de linguagens de programação baseadas em linguagem estruturada TCL e Node.js o Suporte paraSIP (Session Initiation Protocol) sobre MRF (Message Route Framework) e MRF SIP Record Route
• Controle e configuração de persistência de conexão: o Configurável com base em pelo menos: IP de origem, porta de origem, IP de destino, cookies, hash, MSRDP, SIP, cabeçalho HTTP, identificador SSL o Com base em qualquer valor do pacote - incluindo payload - para TCP e UDP o Garantia de afinidade do servidor (direcionando solicitações iniciais e subsequentes de um cliente para o mesmo servidor na farm) o HTTP/2 em modo proxy completo (tanto no lado do cliente quanto no lado do servidor)
• Monitorização da integridade do servidor: o Através de sensores nativos configuráveis pelo menos para: ICMP, TCP, UDP, HTTP/S (analisando a resposta do servidor), WMI, FTP, SMTP, IMAP/POP3, SNMP, DNS, RADIUS, LDAP, SIP, NNTP, SOAP, RPC, SMB, Localização Virtual, WAP, bancos de dados MSSQL/Oracle/MYSQL/PostgreSQL. Assim como o agrupamento de vários sensores através do uso de operadores lógicos. o Com base na execução de scripts para determinar a resposta emulando um cliente o Suporte a monitorização de disponibilidade de serviço HTTP/2
• Programação e automação:

○ Suporte para scripts de programação baseados na linguagem estruturada TCL para configurações fora dos recursos/opções padrão ○ Suporte para extensões Node.js para estender os recursos de Data e Control Plane
• Identificação de falhas em serviços para ações de redundância das aplicações.
• Suporte geolocalização de endereços IP
• Suporte a análise de reputação de IP para evitar conexões de entrada/saída para endereços IP não confiáveis e agrupados em categorias
• Validação de conformidade do tráfego HTTP de acordo com o último RFC do protocolo
• Suporte a 10 conexões de usuários simultâneos para acesso remoto SSL VPN
Suporte obrigatório às seguintes capacidades/features de Web Application Firewall (WAF)
• Proteção de aplicações e serviços Web contra ataques ao nível aplicacional e ataques DOS (Layer 7) de forma proativa (Web Application Firewall) no mesmo dispositivo de balanceamento
• Certificação ICSA como Firewall Aplicacional (WAF)
• Políticas de segurança: ○ Suporte a modo de operação em TCP Reverse Proxy e/ou transparente ○ Suporte a modos de bloqueio ou transparente ○ Suporte de modelos de segurança positivos e negativos ○ Aplicação de políticas por serviço virtual ○ Assinaturas nativas para tecnologias de servidor de mercado (pelo menos Nginx , PHP, Apache, Wordpress e Handlebars) ○ Capacidade de criação de assinaturas personalizadas ○ Suporte para criação automática de políticas, incluindo políticas baseadas em wildcards, com vários URLs ○ Suporte à criação automática de políticas baseadas no comportamento da aplicação e sem intervenção humana ○ Suporte à criação de políticas de segurança para API, através de configuração guiada e importação de um arquivo swagger e OpenAPI ○ Criação e implementação de políticas de segurança, proteção antiBots e proteção contra DoS através de wizards ○ Administração de políticas de segurança por meio de uma API declarativa ○ Suporte para comparar duas políticas e mostrar as diferenças entre ambas ○ Capacidade de personalização de páginas de bloqueio com capacidade de responder a webservices usando um código HTTP 500 ○ Possibilidade de restringir cada um dos seguintes parâmetros: ▪ Protocolo e versão usado ▪ Comprimento do método de request ▪ Comprimento do URI solicitado ▪ Número de cabeçalhos ▪ Comprimento do nome do cabeçalho ▪ Comprimento do valor dos cabeçalhos ▪ Comprimento do payload do pedido ▪ Comprimento do nome e valor do cookie ▪ Número de cookies ▪ Comprimento do nome e valor dos parâmetros ▪ Número de parâmetros ○ Suporte para codificação de idioma multi -byte ○ Validação de URL Encoded Characters
• Programação e automação: ○ Suporte para scripts de programação baseados na linguagem estruturada TCL para configurações fora dos recursos/opções padrão ○ Suporte para extensões Node.js para estender os recursos do plano de dados e do plano de controle da equipe ○ Mecanismos básicos de identificação e proteção: ▪ Top 10 OWASP ▪ Ataques de Brute Force ▪ Cross Site Scripting (XSS) ▪ Cross Site Request Forgery ▪ Injeção SQL

- Parameter e HPP tampering
- Fuga de informações confidenciais
- Session Highjacking
- Buffer Overflows
- Manipulação de cookies
- Encoding attacks
- Broken Access Control
- Forceful Browsing
- Hidden Fields Manipulation
- Request Smuggling
- XML Bombs/DoS
- Open Redirect
- Proteção específica contra ataques HTTP Desync

o Mecanismos avançados de identificação e proteção:
- Criação de assinaturas dinâmicas (de Layer 7), em tempo real, para mitigação de ataques DDoS, incluindo deteção dinâmica de latências do servidor
- Suporte de análise comportamental para mitigação de DDoS (Layer 7) num número ilimitado de serviços
- Proteção contra ataques DDoS, na negociação TLS, mediante Fingerprinting do Stack TLS, apresentada pelo cliente
- Proteção de criptografia de campos confidenciais de aplicações da web no navegador do cliente
- Garantia de integridade dos dados, detctando no mínimo a manipulação de parâmetros em URLs e requests AJAX
- Proteção anti-bot com mecanismos captcha e desafios javascript, para detecção e identificação de navegadores e comportamento do utilizador
- Proteção Web Scraping
- Identificação de URLs com alto consumo em servidores como vetor de ataque DDoS
- Verificação de assinaturas de ataque nas respostas do servidor ao utilizador
- Ofuscação de informações confidenciais enviadas pelo servidor
- Bloqueio com base na localização geográfica (base de dados de geolocalização incluído)
- Drop pacotes, de um IP suspeito, assim que um ataque for detectado
- Verificações de segurança e validação em protocolos FTP e SMTP
- Proteção de XML Web Services e restrição de acesso através de métodos definidos via Web Services Description Idioma (WSDL)
- Suporte de prevenção à exposição de OS Fingerprinting
- Suporte de tecnologias AJAX e JSON
- Dados de reputação de IP que permite que o tráfego de e para endereços IP seja bloqueado em categorias como: scanners , explorações do Windows , negação do serviços , proxies de phishing , botnets e proxies anônimos

o Monitorização, relatórios e diagnósticos:
- Painel de conformidade dos 10 principais OWASP
- Relatórios de conformidade do PCI DSS 3.2
- Possibilidade de captura de tráfego com tcpdump em caso de ataque
- Mecanismos de auditoria de alterações às configurações

o Integrações obrigatórias:
- Integração com ferramentas de verificação de vulnerabilidades (pelo menos WhiteHat, Qualys, IBM AppScan , HP WebInspect.s)
- Integração com servidores Antivirus através do protocolo ICAP
- Integração com bases de dados de Firewalls. Pelo menos IBM InfoSphere Guardium e Firewall de Base de Dados Oracle

licenciamento adicional:

- Capacidade, através de licenciamento adicional, de ativação futura de feeds para proteção contra campanhas de ataque ativo na Internet **e de identificação de aplicações móveis através de integração SDK**

Balanceamento global de funções de DNS

- A solução deve permitir alta disponibilidade de aplicativos distribuídos em 2 ou mais datacenters com, no mínimo, as seguintes características de balanceamento global:

○ Suporte a, pelo menos, os seguintes métodos de balanceamento estáticos e dinâmicos: Round Robin, Disponibilidade Global, Disponibilidade de Aplicativos, Geolocalização, Capacidade do Servidor Virtual, Mínimo de Conexões, Pacotes por Segundo, RTT, Hops, Packet Completion Rate, User-defined QoS, Dynamic Ratio, Ratio, Kilobytes por segundo ○ Suporte de balanceamento dinâmico baseados em QoS: decisões de balanceamento globais avançadas com base na ponderação personalizada pelo utilizador das métricas de desempenho atuais fornecidas automaticamente pelo sistema ○ Persistência em nível global, mantendo os utilizadores no mesmo datacenter durante a sessão ○ Balanceamento de carga de acordo com a localização geográfica ○ Balanceamento de servidores DNS ○ Monitorização de infraestrutura e aplicações, integrando com outros equipamentos do mesmo fabricante ou de terceiros
• Capacidade de funcionar como um servidor DNS autoritativo de alto desempenho, permitindo gerir um domínio inteiro ou uma delegação de parte de um domínio: ○ Suportar, no mínimo, 2 650 000 RPS ○ As zonas DNS autoritativas deverão poder ser carregadas na RAM, para evitar latências e ter tempos de resposta rápidos ○ Suportar cache DNS ○ Incluir ferramenta de administração gráfica para gerir zonas DNS ○ Suporte obrigatório a DNSSEC ○ Suporte a registos AAAA para IPv6 e tradução entre DNS IPv4 e IPv6 ○ Suporte para receber transferências de zona DNS
• Publicação de serviços DNS em anycast
• Capacidade de exibir estatísticas para o serviço DNS, incluindo cache, zonas e recursos DNSSEC
• Suporte a feeds de base de dados de reputação de domínio
Software de gestão
• Software de gestão e repositório/recolha de logs centralizado para todos os componentes e aplicações que possam ser pedidos, mínimo 2000 (componentes + Aplicações)
○ Tem de suportar obrigatoriamente as seguintes capacidades/features: ○ Todos os componentes têm de ser do mesmo fabricante proposto ○ Consola centralizada para monitorização, configuração e descoberta de dispositivos ADC em ambientes on prem/cloud based para dispositivos físicos e/ou virtuais ○ Formato virtual para todos os seus componentes, com suporte os seguintes hipervisores: ▪ VMWare versão mínima 6.X ▪ Hyper-V 2012 ou mais recente ▪ Citrix XenServer versão mínima 6.5 ○ Plataforma de recolha de logs tem que ser separada/independente da plataforma de gestão ○ Plataforma de recolha de dados deverá armazenar todos os alertas, eventos e dados analíticos de cada plataforma gerida ○ Plataforma de gestão deverá ter a capacidade de obter toda a informação necessária (das plataformas de recolha de logs) para efeitos de visibilidade e monitorização ○ Capacidade para gerir centralmente todos os dispositivos (e respetivas *features*), executando operações como backups, gestão de licenças, monitorização, gestão de configurações (como políticas de firewall e políticas de aplicações web) e gestão de aplicações ○ Capacidade de criar e editar objetos de configuração partilhados, como políticas, para implementação desses objetos em vários dispositivos ○ Suporte a RBAC com capacidade de integração com *users* locais, grupos locais, AD, TACACS+, RADIUS e servidores LDAP ○ Capacidade de criação de perfis de autorização baseados em funções e serviços específicos, restringindo funções e permissões para alguns usuários que usam apenas

	uma parte do sistema proposto e defina permissões mais amplas para users administrativos. ○ Capacidade de pesquisa global de objetos (em todas as plataformas geridas) e opção de *drill-down* para obter informação mais detalhada ○ Capacidade de gestão de até 1500 dispositivos através de extensão de licença (de base deve ter licença para um mínimo de 30 dispositivos) ○ Capacidade de visibilidade *end-to-end* para avaliação de parâmetros de performance, disponibilidade e monitorização ○ Capacidade de analítica detalhada, *logging* e de processos de *audit* ○ Capacidade de avaliar o estado de segurança de uma app, round trip time e performance por browser ○ Capacidade de solicitar, importar e gerir certificados (CA-signed SSL certificates, signed SSL certificates e PKCS #12) ○ Capacidade de efetuar push de software para os devices geridos ○ Capacidade de efetuar backups e restores de devices geridos ○ Capacidade de implementação em High Availability ○ Capacidade de automatizar o provisionamento de dispositivos com onboarding declarativo ○ Capacidade de uso de REST APIs declarativas para gerir, provisionar e implementar serviços ○ Capacidade de automatizar a criação, agendamento e exportação de relatórios e alertas ○ Capacidade de analisar políticas, do ponto de vista de segurança, com recurso a um engine de análise de políticas ○ Capacidade de simplificar a gestão de certificados através da automatização nativa de gestão de certificados com Venafi e Let's Encrypt
• Certificação pelo ICSA Labs como um dispositivo IPSEC 1.3	

SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO	
• Serviço de Instalação e Configuração 1 Cluster de balanceadores/Publicadores de Gama Média com instalação na infraestrutura existente.	Chave-na-mão

SERVIÇOS DE ASSISTÊNCIA TÉCNICA PREVENTIVA E CORRETIVA PARA 1 CLUSTER DE BALANCEADORES/PUBLICADORES DE GAMA MÉDIA	
Serviço de operacionalização on site para aplicações críticas (incluindo manutenção de todo o software proposto) para 12 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

Secção II – Instalação, Configuração, Manutenção e Garantia

1. **Nos valores a apresentar, devem estar previstos os seguintes trabalhos de instalação e configuração:**
   i. 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;
   ii. O projeto de instalação deverá ter os seguintes milestones:
      a) Recolha de informação relacionada com o ambiente de produção;
      b) Planeamento para integração com nova estrutura;
      c) Elaboração e desenvolvimento da arquitetura técnica e funcional a implementar, com recomendações de melhorias e melhores práticas;
      d) Planeamento de execução de tarefas para implementação da solução;
      e) Elaboração do High Level Design e Low Level Design;
      f) Planeamento de tarefas para testes de aceitação e validação da solução implementada;
      g) Instalação física de todos os componentes 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 e SAN existentes), Bootup, POST e atualizações para versões de software recomendadas;

h) Testes de failover (redundância física e lógica);
i) Testes de aceitação em cada uma das fases da migração;
j) Colocação, em produção, dos principais serviços definidos pela SPMS - LTM e AWAF (Learn Mode - aprendizagem por aplicação)
k) Colocar AWAF em Alarm Mode e analisar alertas
l) Colocar AWAF em Blocking Mode
m) Planeamento, configuração de solução GTM
n) Testes de aceitação em cada uma das fases da migração
o) Acompanhamento da solução implementada por, pelo menos, 12 meses após o fecho do projeto
p) Todos os trabalhos de planeamento, instalação, configuração, migração e testes têm de ser realizados on-site
q) Entrega de documentação do projeto, passagem de conhecimento, e formação certificada pelo fabricante a 2 elementos da equipa da SPMS
r) Relatório com todas as configurações da solução;

iii. 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:

i. Prazo de mínimo de 3 (três) anos a contar da data de entrega dos equipamentos.

III. 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.

Tendo em conta a prossecução destes princípios, a informação da consulta preliminar é publicitada no portal Internet público da SPMS, da qual faz parte integrante o presente documento, em http://www.spms.min-saude.pt, e no respetivo LinkedIn.

IV. 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 24 de junho de 2024, devendo os interessados indicar claramente no assunto do email a referência "**Consulta Preliminar n.º 09/2024 – Cluster de Balanceadores de Rede".**

V. 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 anexo à presente Consulta Preliminar, devidamente preenchido.

VI. PRAZO DA CONSULTA

A informação prestada pelos operadores económicos será aceite até à data de **24/06/2024.**