

**CONSULTA PRELIMINAR AO MERCADO DAG/DIRS N.º 15/2025****Switches de Core****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 específica 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 em saúde dependem de infraestruturas de rede robustas e seguras, que permitem a cooperação, a partilha de conhecimentos e informação, bem como o desenvolvimento de atividades críticas de prestação de cuidados suportadas pelas tecnologias de informação e comunicação. A rede do SNS desempenha, assim, um papel essencial na transformação digital da saúde, com impacto direto na acessibilidade, eficiência, qualidade e continuidade dos cuidados, bem como na satisfação de profissionais e cidadãos.

À SPMS cabe, ainda, a garantia da operacionalidade, segurança e resiliência das infraestruturas tecnológicas do Ministério da Saúde, promovendo a definição e utilização de normas, metodologias e requisitos que assegurem a interoperabilidade e interconexão dos sistemas de informação da saúde entre si e com os sistemas transversais da Administração Pública. Esse compromisso visa não apenas a modernização tecnológica, mas também a proteção da informação sensível em saúde e a salvaguarda da confiança dos cidadãos.

No âmbito da modernização da rede do SNS, torna-se necessária a aquisição e implementação de switches de core de última geração, capazes de suportar comunicações críticas com elevados requisitos de



resiliência, segurança, redundância e desempenho. Estes equipamentos constituem a espinha dorsal das infraestruturas tecnológicas do SNS, garantindo conectividade contínua e fiável para todos os serviços digitais em saúde. Devem permitir que qualquer entidade do SNS opere num ambiente de rede altamente disponível, seguro e escalável, com administração simplificada e capacidade de evolução tecnológica para responder às necessidades futuras.

II. OBJETIVO

Pretende assim a SPMS, EPE vir a adquirir e instalar os equipamentos necessários à modernização da infraestrutura de rede do Serviço Nacional de Saúde (SNS), nomeadamente switches de core, visando reforçar a resiliência tecnológica, garantir a continuidade dos serviços digitais em saúde e aumentar a capacidade de resposta às crescentes exigências de conectividade, segurança e disponibilidade.

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 e configuração;
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;
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:

Equipamentos e serviços a adquirir

I.	Cluster de Switch de Core (CSC)
II.	Solução de Gestão, Automação e Analítica
III.	Conjunto de Acessórios de Conectividade
IV.	Serviços de instalação, configuração dos equipamentos e plataforma de gestão
V.	Serviços de Assistência Técnica Preventiva e Corretiva durante o período de 36 meses com cobertura 24 x 7 com 4 horas de tempo de resposta para os equipamentos referidos no ponto I.

Deve ser assegurado o seguinte:

- 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>.
- Cumprir o estipulado na Resolução do Conselho de Ministros nº 132/2023, disponível em <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/132-2023-223267497>

3.1. PRESSUPOSTOS E ARQUITETURA DE REDE DA SOLUÇÃO

A arquitetura da solução deverá cumprir as seguintes premissas:

- A solução deverá garantir plena interoperabilidade, podendo ser mono ou multi-fabricante, desde que certificada pelo fornecedor responsável;
- Toda a solução de gestão deverá ser em formato de appliances virtuais, sendo que o software deverá funcionar sobre os hypervisors VMWare, HyperV ou equivalente. Em ambas as abordagens, é obrigatório que a arquitetura de alta disponibilidade atenda aos seguintes requisitos:
 - Redundância local: Funcionamento em cluster totalmente redundante no modo ativo-ativo ou ativo-passivo;
 - Gestão local: Cada appliance virtual deve providenciar uma gestão centralizada do cluster CSC, permitindo o controlo granular sobre os mecanismos de alta disponibilidade referidos na secção 3.3.



3. Devem ser fornecidas todas as ligações de interligação entre os dois chassis de core, incluindo transceivers, cablagem e quaisquer elementos passivos/ativos necessários, homologados pelo fabricante.
4. Devem dimensionar e fornecer as ligações de interligação entre os dois chassis de core, com base nas seguintes premissas:
 - a. A capacidade mínima da interligação entre chassis de core deve ter capacidade mínima equivalente a 120% da maior das seguintes situações:
 1. A soma das uplinks externas de um chassis;
 2. O maior débito agregado de acesso que possa atravessar a interligação em caso de falha de um dos chassis.
 - b. Agregação/Redundância (LAG/MLAG/ECMP) sem pontos únicos de falha, com n+1 e headroom $\geq 30\%$ de utilização média;
 - c. Todos os links de cada agregação devem ter a mesmo débito nominal e latência equivalente;
 - d. Deve ser fornecida justificação do dimensionamento, baseada no cálculo do débito considerado, incluindo perfis de tráfego, oversubscription e cenários de falha.
5. A solução a apresentar deverá disponibilizar uma gestão centralizada a nível de cada cluster de core, garantindo segregação entre clusters. Cada cluster deverá dispor da sua própria appliance virtual, instalada em cada site (LAN).
6. A solução deverá ser implementada exclusivamente em ambiente de alojamento proprietário, não sendo aceitáveis arquiteturas em cloud pública;
7. Deverá ser apresentado um documento com a arquitetura física e lógica de alta disponibilidade proposto pelo ADJUDICATÁRIO.
8. Os operadores deverão indicar os modelos de licenciamento disponíveis, nomeadamente perpétuo, subscrição ou híbrido de com as especificações técnicas do ponto 3.3.



3.2. MAPA DE QUANTIDADES

Componente Geral			
Ponto	Descrição	Quantidade	
I.	Clusters de core L2/L3 modelares	80	
II.	Solução de Gestão, Automação e Analítica	80	
Componente por equipamento (chassi)			
Ponto	Descrição	Quantidade	
I.	Cartas supervisoras/gestão	>= 1	
	Placas de interface de rede (line cards)	>= 2	
	Unidades de arrefecimento (ventoinhas)	>= 4	
	Fontes de alimentação	>= 4	
II.	Solução virtualizada de Gestão, Automação e Analítica	>= 1	
Componente de placas de interface de rede: Opção-1			
Ponto	Descrição	Quantidade	
I.	Interfaces Ethernet 1/10Gbps com conector RJ45 (8P8C)	>= 2	
	Interfaces Ethernet SFP 10/25 Gbps	>= 2	
	Interfaces Ethernet QSFP 40 Gbps		
	Interfaces Ethernet QSFP28 100 Gbps		
Componente de placas de interface de rede: Opção-2			
Ponto	Descrição	Quantidade	
I.	Interfaces Ethernet 1/10Gbps com conector RJ45 (8P8C)	>= 2	
I.	Interfaces Ethernet SFP 10/25 Gbps	>= 2	
	Interfaces Ethernet QSFP 40 Gbps	>= 2	
	Interfaces Ethernet QSFP28 100 Gbps		
Componente de interface de rede e carta supervisora: Opção-3			
Ponto	Descrição	Quantidade (line cards)	Quantidade interfaces por carta supervisora/gestão
I.	Interfaces Ethernet 1/10Gbps com conector RJ45 (8P8C)	= 2	N/A
	Interfaces Ethernet SFP 10/25 Gbps	>= 2	N/A
	Interfaces Ethernet QSFP 40 Gbps		= 2
	Interfaces Ethernet QSFP28 100 Gbps		= 2
Conjunto de Acessórios de Conectividade			
Ponto	Descrição	Quantidade	
III.	Módulos SFP+ 10GBASE-LR 1310nm 10km Duplex LC SMF DOM	3072	
	Módulos SFP+ 10GBASE-SR 850nm 300m Duplex LC MMF DOM	768	



3.3. CARACTERÍSTICAS TÉCNICAS

I. Cluster de Switch de Core (CSC)	
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 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	
Número mínimo de interfaces por placa de rede	
• Interfaces Ethernet 1/10Gbps com conector RJ45 (8P8C)	>= 24
• Interfaces Ethernet SFP 10/25 Gbps	>= 20
• Interfaces Ethernet QSFP28 40 Gbps	>= 2
• Interfaces Ethernet QSFP28 100 Gbps	>= 2
Características Físicas	
• Equipamento modular ethernet L2/L3	>= 4 RU
• Número de slots suportadas	>= 4
• Fontes de alimentação redundantes, removíveis em operação (hot-swappable)	>= 4
• As fontes de alimentação requerem certificação mínima de 80 Plus ou equivalente, isto é, devem possibilitar uma eficiência energética mínima de 80% em cargas de 20%, 50% e 100%, respetivamente	>= 80%
• Capacidade para 2 slots dedicadas a cartas supervisoras/gestão	>= 1
• Capacidade para 4 slots dedicadas a módulos de interfaces de rede (line cards)	>= 4
• Suporte de portas de gestão Ethernet do tipo RJ45 a 1G ou 10G com encaixe SFP	>= 1
• Suporte de portas USB	>= 1
• Valor máximo de Acústica (LwA)	8.3 Bels
• Certificação ambiental: RoHS, REACH, Energy Star, ou equivalente	Obrigatório
• MTBF mínimo expresso em horas	>= 100 000 h
Escalabilidade e Performance	
• Capacidade comutação do sistema	9,6 Tbps
• Capacidade mínima de transferência por slot	480 Gbps
• Capacidade encaminhamento	>= 2 Bpps
• Número mínimo de MAC Addresses suportados	32 000
• Número mínimo de rotas suportadas	>= 65 536
• Suporte de MACSec com encriptação	>= 128 bits
• Número mínimo de VLAN ID's	>= 4090
• Número mínimo de instâncias STP	1000
• Número mínimo de VRFs suportadas	>= 256
Funcionalidades, Protocolos e Tecnologias	
- Suporte de Fontes de alimentação AC e DC - Automatic Medium-Dependent Interface Crossover (auto-MDIX) - Suportar LLDP	



- Suportar DHCP Server
- Suporte de DHCP Relay
- Suporte de LACP com um mínimo de agregação de 8 links
- Suporte de LACP multi-slot/linecard
- O sistema deverá suportar mecanismos de redundância e agregação multi-chassis (MC-LAG ou equivalente) permitindo a ligação redundante em ativo-ativo entre dois chassis distintos, com deteção rápida de falha
- Suporte de extensões: Bridge Protocol Data Unit (BPDU), BPDU guard, BPDU filtering, bridge assurance, loop guard, e root guard;
- Permitir MAC addresses estáticos
- Suporte de Q-in-Q
- Capacidade de Selective Q-IN-Q ou Vlan Mapping
- Suporte para IPv4 em Hardware
- Suporte de Jumbo Frames
- Suporte para IPv6 em Hardware
- Suporte para 8 egress queues por porta (QoS)
- Suporte de ACLs de Layer-2 e Layer-3 em IPv4 e IPv6
- Capacidade de Suporte de Port Based ACLs IPv4 e IPv6
- Suporte para DAI (Dynamic ARP inspection)
- Suporte para Port security
- Suporte de RSTP, STP, MSTP
- Suporte de VRRP
- Suporte de HQoS e WRED nativamente
- Implementar CBWFQ em todas as portas
- Possuir mecanismos de proteção do Control Plane
- Capacidade de Suporte de IP SLA ou equivalente (Probe-Based Monitoring)
- Suportar rotas estáticas IPv4 e IPv6
- Suportar RIPv2 (IPv4) e RIPv6 (IPv6)
- Suportar OSPFv2 e OSPFv3
- Suportar BGP
- Suportar Equal Cost Multipath Routing (ECMP)
- Suporte de Inter-vlan routing
- Implementar PBR (Policy-Based Routing)
- Suportar BFD (Bidirectional Forwarding Detection)
- Suporte de túneis GRE (Generic Routing Encapsulation)
- Suportar MPLS Layer 3 VPNs
- Suportar BGP EVPN sobre VXLAN
- Suportar VRF e VRF-Lite
- Suportar VXLAN
- Suportar NETCONF e YANG
- Suportar Gestão Web (HTTPS)
- Permitir captura de fluxos de tráfego em formato IPFIX ou similar
- Suportar o uso do Interior Gateway Management Protocol (IGMPv2 e v3)
- Suportar PIM Stub, PIM SM e PIM SSM
- Suportar SSHv2
- Suportar SNMPv2 e SNMPv3
- Suporte de Syslog
- Suportar 802.1X
- Suporte para 802.1X com Change of Authorization (CoA)



- Suporte para 802.1X com Downloadable ACLs (dACLs)
- Suporte para 802.1X com Guest VLAN
- Suporte para RADIUS Authentication, Authorization e Accounting
- Suporte para TACACS Authentication, Authorization e Accounting
- Suporte de funcionalidades de segurança para defesa da integridade do hardware e software do switch, nomeadamente:
 - i. Assinatura de imagens para garantir a autenticidade da imagem de software
 - ii. Boot seguro do equipamento assente em chip de hardware imutável

Standards – Normas e especificações

- Interfaces Ethernet RJ45 1/10Gbps – IEEE 802.3ab, IEEE 802.3an
- Interfaces Ethernet SFP 10 Gbps – IEEE 802.3ae
- Interfaces Ethernet SFP28 25 Gbps – IEEE 802.3by
- Interfaces Ethernet QSFP28 40 Gbps – IEEE 802.3ba
- Interfaces Ethernet QSFP28 100 Gbps – IEEE 802.3ba
- Suporte de MACSec com encriptação – IEEE 802.1AE
- LLDP – IEEE 802.1AB
- DHCP Server – RFC 2131
- DHCP Relay – RFC 1542
- LACP – IEEE 802.3ad
- Q-in-Q – IEEE 802.1ad, IEEE 802.1Q
- Selective Q-in-Q / Vlan Mapping – IEEE 802.1ad, IEEE 802.1Q
- IPv4 em Hardware – RFC 791
- IPv6 em Hardware – IEEE 802.3, RFC 8200
- QoS – 8 egress queues – IEEE 802.1p
- RSTP, STP, MSTP – IEEE 802.1w, IEEE 802.1D, IEEE 802.1s
- VRRP – RFC 2338 RFC 5798
- HQoS e WRED – IEEE 802.1p, RFC 2309, RFC 2697–2698
- CBWFQ – RFC 2475
- Rotas estáticas IPv4 e IPv6 – RFC 791, RFC 8200
- RIPv2 IPv4 e RIPv6 – RFC 2453, RFC 2080
- OSPFv2 e OSPFv3 – RFC 2328, RFC 5340
- BGP – RFC 4271
- ECMP – RFC 2992
- Inter-vlan routing – IEEE 802.1Q
- PBR Policy-Based Routing – RFC 1102
- BFD – RFC 5880–5881
- Túneis GRE – RFC 2784
- MPLS Layer 3 VPNs – RFC 4364
- BGP EVPN sobre VXLAN – RFC 7432
- VXLAN – RFC 7348
- NETCONF e YANG – RFC 6241, RFC 7950
- Gestão Web HTTPS – RFC 2818
- IPFIX – RFC 7011–7015
- IGMPv2 e v3 – RFC 2236, RFC 3376
- PIM Stub, PIM SM, PIM SSM – RFC 4601, RFC 3569
- SSHv2 – RFC 4251–4254

Resiliência e Alta disponibilidade



- Suportar os modos de operação:
 - Ativo-Ativo
 - Ativo-passivo
- 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
- Suporte a PIM com múltiplos Designated Routers (Dual DR) ou equivalente para redundância multicast
- Ligação entre chassis ou switches (Inter-Switch Link) para agregação e resiliência
- Capacidade de encaminhamento ativo/ativo entre chassis ou dispositivos redundantes
- Suporte a gateway ativo/ativo (VIP, VMAC, multinetting)
- Configuração de link-up delay para deteção rápida de falhas e reconvergência

II. Solução de Gestão, Automação e Analítica

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 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 Cluster de Equipamentos

Funcionalidades de Orquestração e Gestão

- | | |
|---|-------------|
| • Disponível em appliance virtualizada OVA/OVF (VMware), QCOW2 (KVM) | Obrigatório |
| • Interface única para gestão de switches/core/fabric | |
| 1. Definição central de políticas (QoS, ACL, segurança, segmentação) | |
| 2. Suporte a APIs abertas (REST, NETCONF, YANG, gNMI) para integração com orquestradores externos | |
| 3. Exportação em tempo real (streaming telemetry) para monitorização e analítica | |
| 4. Monitorização com AI/ML para detetar anomalias, prever falhas e sugerir otimizações | |
| 5. Identificação e análise de tráfego na camada aplicacional (Layer-7) | |
| 6. Gestão de overlays/underlays (VXLAN, EVPN, MPLS) | Obrigatório |
| 7. Capacidade de gerir múltiplos datacenters/sites de forma unificada | |
| 8. Segmentação dinâmica, integração com NAC/AAA e políticas contextuais | |
| 9. Dashboards gráficos e relatórios de desempenho, falhas e segurança | |

Standards – Normas e especificações

1. IEEE 802.1Q, IEEE 802.1p, RFC 2474, RFC 4007
2. RFC 6241, RFC 6020, OpenConfig (gNMI)
3. RFC 8641, gRPC (IETF drafts), RFC 7011
4. RFC 7348, RFC 7432, RFC 3031
5. RFC 7011, RFC 8329
6. RFC 7348, RFC 7432, RFC 3031



7. MEF 70.1 (LSO)
8. IEEE 802.1X, RFC 2865, TACACS+, SAML 2.0
9. RFC 5424, RFC 3411

Características de operacionalização centralizada

- Monitorização de CPU, memória, consumo de energia, temperatura e interfaces, com armazenamento de informações históricas.
- Estado atual de fim de suporte de software e hardware com perspetiva de 18 meses; visibilidade detalhada do inventário de software e hardware em produção ou próximo de produção
- Notificações automáticas sobre vulnerabilidades e outros problemas relacionados com a segurança, bem como avisos de fim de suporte de hardware e software
- Visualização do nível de rede, incluindo switches de core, interfaces e endpoints, com representação clara do inventário
- Suporte a arquiteturas com múltiplos clusters, permitindo gestão centralizada e agregada
- Gestão de acessos diferenciados, syslog, registos de auditoria, backups e gestão de recursos de forma integrada
- Notificações sobre hardware e software, recomendações de melhores práticas e alertas de sustentabilidade
- Identificação de bugs suscetíveis e ativos na rede para suporte proativo à manutenção
- Alertas sobre anomalias de conectividade, configuração, hardware, capacidade e bugs ativos
- Capacidade de integrar e monitorizar serviços DNS para gestão da rede
- Identificação de latência, congestionamento e falhas de rede através da análise de tráfego por aplicação

3.4. SERVIÇOS DE INSTALAÇÃO, MANUTENÇÃO E SUPORTE

IV. Serviços de Instalação, configuração dos equipamentos e plataforma de gestão

Serviços para pontos I, II, III

Requisitos

1. Os equipamentos devem ser instalados e configurados de acordo com as boas práticas do fabricante.
2. 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 dos equipamentos e da solução de gestão;
 - 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 infraestrutura de switching, firewalls, servidores, ou outros equipamentos existentes). Deve ainda contemplar o processo de arranque dos equipamentos (bootup), a execução do autoteste de hardware (POST) e a atualização para as versões de software recomendadas pelo fabricante.
 - h) Relatório com todas as configurações da solução;



V. Serviços de Assistência Técnica Preventiva e Corretiva

Serviços para pontos I, II

Requisitos – Operacionalização e Manutenção dos equipamentos

1. Atualização de firmwares que suportam o correto e seguro funcionamento destes equipamentos
2. Em caso de avaria, mau funcionamento ou anomalia de qualquer componente hardware, esta deverá ser substituída por componentes de hardware originais e certificados pelo fabricante
3. Manutenção de todo o firmware de suporte aos equipamentos em contrato de manutenção, bem como do software necessário para o seu correto funcionamento:
 - a) Disponibilização de todas as atualizações, correções e ajustes do firmware ou software para os equipamentos
 - b) Tudo o que for disponibilizado deverá estar certificado pelo fabricante do equipamento em causa
4. Os serviços de reparação deverão ser realizados apenas por técnicos de equipas residentes em Portugal e devidamente credenciados pelo fabricante do equipamento
5. 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
6. 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
7. Declaração do fabricante onde conste o conhecimento técnico da infraestrutura e responsabilidade pela solução apresentada na proposta

Requisitos – Níveis de Serviço

Os valores apresentados são de referência

1. Horário de cobertura: 24 horas, 7 dias por semana	24 horas, 7 dias por semana
2. O suporte com início em chamada telefónica deverá ter os seguintes requisitos	
a) Problemas críticos com indisponibilidade ou degradação de serviço resultante de avaria, mau funcionamento ou anomalia de qualquer dos componentes descritos nesta consulta	30 minutos
b) Problemas não críticos, que não gerem indisponibilidade, mas que identifiquem uma avaria, mau funcionamento ou anomalia de qualquer dos componentes descritos na clausula anterior	120 minutos
3. Sendo necessária a intervenção física no local, esta deverá ser dado o cumprimento aos seguintes requisitos:	
a) Problemas críticos com indisponibilidade ou degradação de serviço resultante de avaria, mau funcionamento ou anomalia de qualquer dos componentes descritos nesta consulta	120 minutos
b) Problemas não críticos, que não gerem indisponibilidade, mas que identifiquem uma avaria, mau funcionamento ou anomalia de qualquer dos componentes descritos na clausula anterior	NBD (next business day)

Garantia

1. Nos termos da presente Cláusula e da lei que disciplina os aspetos relativos à venda de bens de consumo e das garantias a ela relativas a empresa garante os bens objeto do contrato, pelo prazo de mínimo de 36 (trinta e seis) meses a contar da data de entrega dos equipamentos



2. Todos os produtos deverão estar sujeitos a uma garantia do fabricante, com suporte de 36 (trinta e seis) meses e, caso aplicável, o software a ele adstrito será originalmente licenciado para a SPMS, EPE.
3. A ENTIDADE PÚBLICA 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>, no respetivo LinkedIn e **plataforma eletrónica de contratação** www.comprasnasaude.pt, devendo os operadores económicos interessados em apresentar contributos no âmbito da presente Consulta Preliminar, **remeter os seus contributos através da plataforma eletrónica de contratação** www.comprasnasaude.pt, cuja ref.ª é **2025/57**, no prazo de 15 dias úteis, contando com o dia da sua publicação.

V. PRESTAÇÃO DE INFORMAÇÃO PELOS OPERADORES ECONÓMICOS

A prestação voluntária de informação pelos operadores económicos, deverá ser efetuada **através da plataforma eletrónica de contratação** www.comprasnasaude.pt, cuja ref.ª é **2025/57**, no prazo de 15 dias úteis, contando com o dia da sua publicação.

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 no prazo de 15 dias úteis, contando com o dia da sua publicação.