CONSULTA PRELIMINAR AO MERCADO DAG/DIRS N.º 18/2025

Soluções de Backup On-Premise para Ambientes Microsoft 365 e Google Workspace

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 a SPMS, EPE, recolher contributos do mercado para a futura contratação de uma solução de backup on-premise destinada a proteger os dados das principais ferramentas das plataformas de colaboração Microsoft 365 (M365) e Google Workspace (GWS) em uso no SNS.

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 detalhadas sobre as soluções disponíveis que cumpram os requisitos técnicos, funcionais e de licenciamento descritos neste documento.

Com a presente consulta, pretende-se identificar:

- O preço base a considerar pela entidade adjudicante face à solução pretendida, para cada um dos cenários e requisitos definidos.
- A viabilidade e os modelos de licenciamento perpétuo disponíveis no mercado.
- Estruturas de custo detalhadas, incluindo modelos de TCO (Custo Total de Propriedade).
- Arquiteturas de referência capazes de suportar os volumes de dados e o número de utilizadores do SNS.
- Exibição de outros cenários e considerações relevantes no âmbito dos serviços identificados.

A consulta preliminar será constituída por:

1. DESCRIÇÃO GERAL DA SOLUÇÃO PRETENDIDA

1.1. Contexto e Serviços a Proteger

A solução de backup on-premise destina-se a proteger os dados das plataformas Microsoft 365 e Google Workspace em uso no SNS. A cobertura obrigatória inclui, no mínimo, os seguintes serviços:

Microsoft 365:

- Exchange Online (incluindo Calendário e Caixas Partilhadas).
- OneDrive.
- SharePoint.

- Teams (contexto completo da aplicação: ficheiros, conversas, metadados, configurações, permissões, tabs, wikis e dados de aplicações integradas como Planner e Copilot).
- Forms.
- Entra ID.

Google Workspace:

- Gmail (incluindo Calendário).
- Drive.
- Shared Drives.
- Forms.
- Meet (Gravações e conversas).

1.2. Âmbito e Cenários de Dimensionamento

A solução deve ser dimensionada para os seguintes três cenários, considerando um ambiente híbrido onde os utilizadores podem migrar entre M365 e GWS durante o contrato. O volume de dados tem uma previsão de crescimento de 10% ao ano.

- **Cenário 1**:
  - Utilizadores: 200.000 colaboradores.
  - Email/Gmail: 800 TB de Storage.
  - SharePoint: Mínimo de 300 TB.
  - OneDrive e Google Drive: 60 PB.
  - Teams: Mínimo de 60.000 equipas.
  - Google Shared Drives: Mínimo de 10.000.
- **Cenário 2:**
  - Utilizadores: 150.000 colaboradores.
  - Email/Gmail: 600 TB de Storage.
  - SharePoint: Mínimo de 300 TB.
  - OneDrive e Google Drive: 52 PB.
  - Teams: Mínimo de 40.000 equipas.

- Google Shared Drives: Mínimo de 10.000.

- **Cenário 3**:
  - Utilizadores: 10.000 colaboradores.
  - Email/Gmail: 500 TB de Storage.
  - SharePoint: Mínimo de 300 TB.
  - OneDrive e Google Drive: 45 PB.
  - Teams: Mínimo de 30.000 equipas.
  - Google Shared Drives: Mínimo de 10.000.

2. REQUISITOS TÉCNICOS E FUNCIONAIS

2.1. Modelo de Licenciamento e Custos

- **Licenciamento Perpétuo**: É um requisito explícito a preferência por um modelo de licenciamento perpétuo. Os operadores devem confirmar a disponibilidade deste modelo. Caso não seja a oferta principal, devem detalhar como pode ser adquirido e quais as suas limitações, numa perspetiva de 10 anos.

- **Estrutura de Custos**: A proposta deve discriminar se a estrutura de custos é baseada no número de utilizadores, na capacidade de armazenamento, ou num modelo híbrido. Deve clarificar inequivocamente como o custo escala com o volume de armazenamento para consumos que excedam quotas por utilizador.

- **TCO:** Deve ser fornecido um modelo ou calculadora para estimar o TCO, incluindo custos de software, hardware, manutenção e operacionais.

2.2. Direitos de Acesso aos Dados Pós-Contrato

- A garantia de acesso perpétuo aos dados de backup, mesmo após o término da relação comercial, é um requisito não negociável.

- No modelo perpétuo, o software existente deve continuar a funcionar e o acesso aos dados para recuperação deve permanecer totalmente funcional, mesmo que o contrato de suporte expire.

- Qualquer proposta deve incluir uma cláusula que garanta a funcionalidade de recuperação de dados de forma perpétua ou, em alternativa, forneça ferramentas para a exportação em massa de todos os dados para um formato aberto antes do final do contrato.

2.3. Capacidades de Recuperação e eDiscovery

- **Recuperação Granular**: A solução deve permitir a recuperação de itens individuais (ex: um email, , uma mensagem no Teams) sem necessidade de restaurar o repositório completo (ex: a caixa de correio inteira).
- **Recuperação em Massa:** A solução deve dispor de ferramentas robustas para a recuperação em massa de múltiplos utilizadores, sites ou caixas de correio em simultâneo
- **Retenção Legal (Legal Hold):** Deve ser possível marcar e preservar dados específicos indefinidamente para fins de investigação, sobrepondo-se às políticas de retenção normais.
- **eDiscovery:** A solução deve funcionar como um arquivo pesquisável, permitindo pesquisas complexas em todos os dados de backup com base em palavras-chave e metadados.

2.4. Arquitetura da Solução

- Os operadores devem apresentar uma proposta de arquitetura robusta, distribuída e escalável para uma implementação on-premise dos volumes de dados indicados. A proposta deve detalhar as 3 camadas lógicas: Gestão, Processamento e Armazenamento.
- Deve ser apresentado o dimensionamento de hardware e a previsão de *storage*, incluindo o cálculo da capacidade de armazenamento em bruto para períodos de retenção de 2, 4 e 6 anos.

2.5. Framework de Segurança Integrada

- **Encriptação:** A solução deve encriptar os dados em trânsito.
- **Imutabilidade:** Os backups devem ser imutáveis, não podendo ser alterados, encriptados ou eliminados até o período de retenção expirar. A proposta deve indicar se esta funcionalidade é baseada em software ou hardware.
- **Controlo de Acessos:** A solução deve ter um controlo de acessos granular por função e permitir a integração com AD/Entra ID, com exigência de autenticação multifator (MFA) para acesso à consola de gestão.

2.6. Modelos de Suporte e Conformidade

- **Suporte e SLAs:** Descrever os modelos de suporte disponíveis, com foco em suporte 24x7x365, e especificar os SLAs para o tempo de resposta em incidentes críticos.
- **Conformidade Regulatória:** Demonstrar a conformidade da solução com o Regulamento Geral sobre a Proteção de Dados (GDPR).
- **Certificações de Segurança:** Apresentar certificações relevantes como ISO/IEC 27001, SOC 2, etc.

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.

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 **2025/61**, no prazo de 15 dias úteis, contando com o dia da sua publicação.

IV. 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 **2025/61**, no prazo de 15 dias úteis, contando com o dia da sua publicação.

V. INFORMAÇÃO PRETENDIDA

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

1. **Proposta de Preços:** Apresentação de uma estimativa de custos detalhada para cada um dos três cenários de dimensionamento, discriminando o modelo (por utilizador, por capacidade, etc.).
2. **Modelo de Licenciamento:** Confirmação explícita sobre a disponibilidade de licenciamento perpétuo e detalhe das condições. Apresentar alternativas caso o modelo perpétuo não esteja disponível.
3. **Custo Total de Propriedade (TCO):** Fornecimento de um modelo de TCO que permita à SPMS estimar os custos totais a 5 e 10 anos, incluindo hardware, software, manutenção e custos operacionais.
4. **Arquitetura e Dimensionamento:** Apresentação de uma arquitetura de referência para o Cenário 1, com o detalhe das camadas de gestão, processamento e armazenamento, e uma estimativa do hardware necessário.
5. **Segurança e Conformidade:** Descrição detalhada de como a solução cumpre os requisitos de encriptação, imutabilidade e controlo de acessos. Apresentar comprovativos de conformidade com o GDPR e certificações de segurança (ex: ISO 27001).
6. **Acesso Pós-Contrato:** Clarificação contratual sobre a garantia de acesso e funcionalidade de restauro dos dados em caso de expiração de contrato de suporte (para licenças perpétuas) ou término de subscrição.
7. **Modelos de Suporte:** Descrição dos níveis de suporte disponíveis, com detalhe dos SLAs para incidentes críticos (24x7x365).

8. **Outras Considerações:** Quaisquer outras informações ou cenários que o operador económico considere relevantes para o objeto desta consulta.

VI. PRAZO DA CONSULTA

A informação prestada pelos operadores económicos será aceite no prazo de 15 dias úteis, contando com o dia da sua publicação.