CONSULTA PRELIMINAR

"Migração para a Cloud e implementação Lisboa DataHub"

CÂMARA MUNICIPAL DE LISBOA
Departamento de Sistemas de Informação

LISBOA

1. Índice

2. ENQUADRAMENTO

O Município de Lisboa, na qualidade de Entidade Adjudicante e através do Departamento de Sistemas de Informação, realiza por via desta comunicação, uma consulta preliminar ao mercado, consulta essa que se fundamenta no artigo 35º-A do Código dos Contratos Públicos, na sua versão atual.

A consulta preliminar ao mercado é um processo fundamental no âmbito da contratação pública, que visa antecipar o procedimento formal de adjudicação e promover uma abordagem mais informada e estratégica.

Este mecanismo permite à entidade contratante obter uma visão detalhada sobre o mercado disponível, as alternativas técnicas, as soluções inovadoras e as estimativas de custos associadas aos bens ou serviços que pretende adquirir, antes de lançar o procedimento formal de contratação.

3. FORMA DA CONSULTA

É imperativo que esta 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. Com esse objetivo em vista, toda a informação da consulta preliminar é publicitada no portal Internet público da Câmara Municipal de Lisboa - https://www.lisboa.pt/.

A prestação voluntária e não vinculativa de informação pelos operadores económicos deverá ser feita através do endereço de e-mail dsi.cp@cm-lisboa.pt até às 24h do dia 13 de fevereiro de 2026.

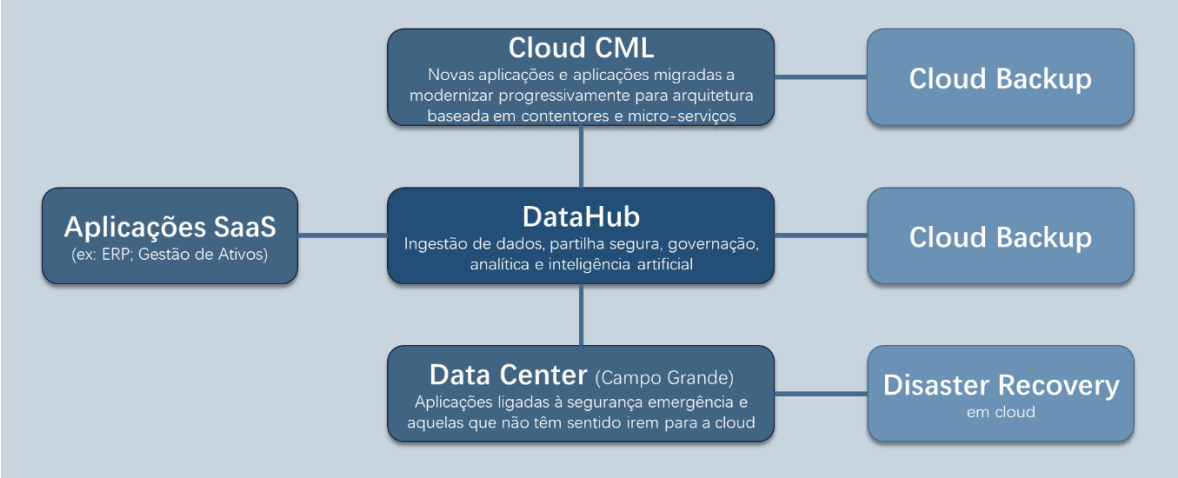
4. OBJETO DA CONSULTA - ESPECIFICAÇÕES

A transformação digital da administração pública é um vetor essencial para a modernização dos serviços prestados aos cidadãos e para a melhoria da eficiência interna das organizações. Neste contexto, a Câmara Municipal de Lisboa (CML) reconhece a necessidade de dotar-se de infraestruturas tecnológicas modernas, escaláveis e seguras, que sustentem a crescente

complexidade dos seus sistemas de informação e a intensificação do uso de dados na tomada de decisão.

Pretende-se implementar uma estratégia de modernização tecnológica baseada numa infraestrutura híbrida — combinando recursos on-premises e serviços em cloud — para maximizar a eficiência dos investimentos públicos, reforçar a segurança dos sistemas críticos e acelerar a inovação.

A adoção de uma **plataforma Cloud** permitirá à CML garantir maior **flexibilidade**, **escalabilidade** e **resiliência**, reduzindo a dependência de infraestruturas físicas na sua responsabilidade e promovendo uma gestão mais eficiente dos recursos tecnológicos. Por sua vez, a implementação de um **DataHub municipal** será fundamental para centralizar, integrar e explorar dados de forma segura e eficaz, promovendo a interoperabilidade entre sistemas e apoiando a tomada de decisão baseada em dados.



Relação entre os diversos componentes da infraestrutura de sistemas de informação que se pretende para a CML

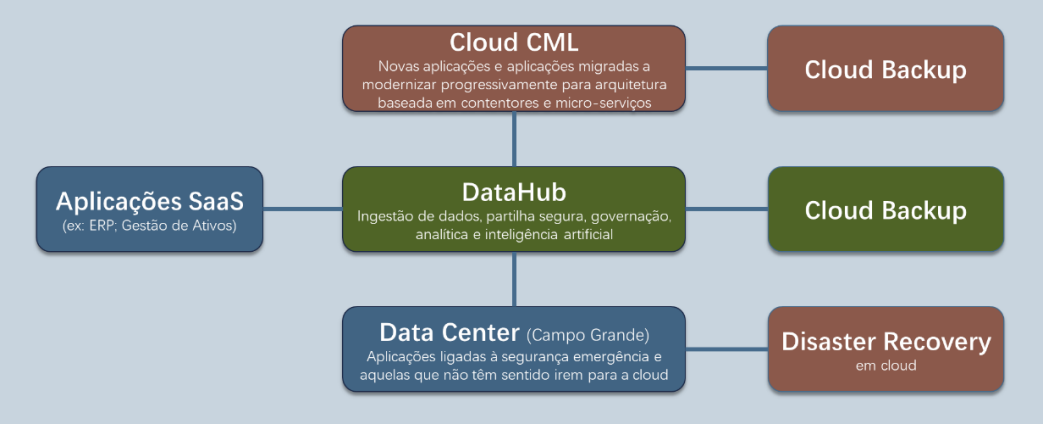
Pretende-se evoluir para uma arquitetura composta por quatro pilares complementares: (i) **Cloud CML**, dedicada a novas aplicações e à modernização das aplicações migradas, com adoção progressiva de contentores e micro-serviços; (ii) **Lisboa DataHub**, plataforma central de ingestão, partilha segura, governação, analítica e inteligência artificial; (iii) **Data Center da CML**, para aplicações ligadas à segurança/emergência e outras que não se justifique migrar; e (iv) capacidades transversais de resiliência, nomeadamente **Cloud Backup** (para Cloud CML e DataHub) e **Disaster Recovery** em cloud para cargas críticas do Data Center, garantindo redundância geográfica, replicação assíncrona dos dados, políticas de failover automatizado e tempos de recuperação compatíveis com os objetivos de RPO (Recovery Point Objective) e RTO (Recovery Time Objective) definidos.

No âmbito desta consulta preliminar, a CML solicita informação considerando dois modelos

distintos:

Modelo A — Sistema Cloud CML e sistema DataHub em fornecedores de cloud diferentes.

Pretende-se a implementação de plataformas autónomas em clouds distintas, assegurando interoperabilidade, governação e segurança entre domínios, sem comprometer a portabilidade de dados e serviços.



*A castanho e verde as duas componentes a considerar em separado no **Modelo A** (hipótese de cada uma dessas componentes ser assegurada por fornecedores distintos)*

SISTEMA CLOUD CML

Inclui-se aqui a migração para cloud da infraestrutura atualmente on-premises, o Disaster Recovery para as aplicações de emergência e segurança e sistemas de suporte à Plataforma de Gestão Inteligente de Lisboa (PGIL) que ficam on-premises e o cloud backup das aplicações em cloud.

A solução deve incluir mecanismo de backup para uma infraestrutura distinta da principal.

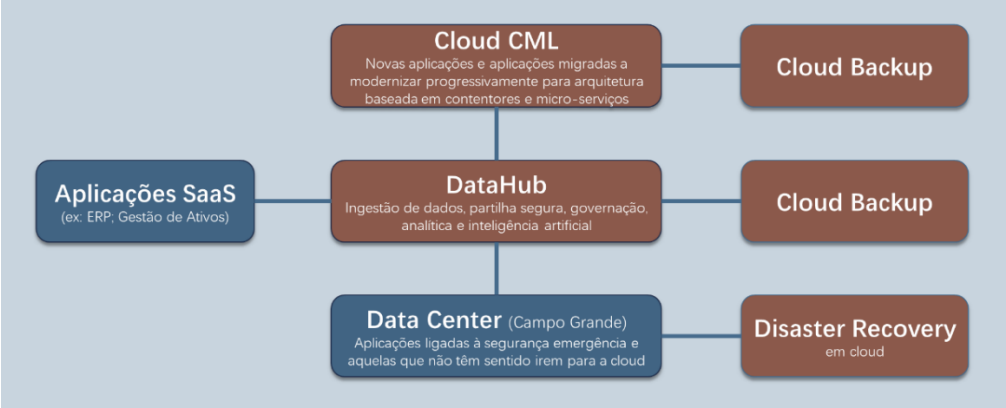
SISTEMA DATAHUB

Inclui-se aqui a implementação do DataHub e da Cloud Backup do DataHub.

A solução deve incluir mecanismo de backup para uma infraestrutura distinta da principal.

Modelo B — Sistema Cloud CML e Sistema DataHub no mesmo fornecedor de cloud.

Implementação integrada das duas plataformas no mesmo ecossistema de cloud, explorando eventuais sinergias técnicas, operacionais e financeiras.



*A castanho o que se inclui no **Modelo B** (hipótese de as duas componentes serem disponibilizadas por um único fornecedor)*

Inclui:

- a migração para cloud da infraestrutura atualmente on-premises, o Disaster Recovery para as aplicações de emergência e segurança e sistemas de suporte à Plataforma de Gestão Inteligente de Lisboa (PGIL) que ficam on-premises e o cloud backup das aplicações em cloud.
- Inclui a implementação do DataHub e da Cloud Backup do DataHub.

  A solução deve incluir mecanismos de backup para uma infraestrutura distinta da principal.

A CML pretende obter uma avaliação comparativa dos dois modelos, nomeadamente nos seguintes eixos:

1) **Custos e modelos de licenciamento** (TCO – Total Cost of Ownership a 4 anos)
   - Visão consolidada dos custos de implementação, operação, suporte, manutenção, formação e transferência de conhecimento, permitindo comparar sinergias do fornecedor único com eventuais ganhos de concorrência em fornecedores distintos.
2) **Tecnologia e arquitetura**
   - Enquadramento das arquiteturas propostas, serviços e padrões/formatos

(privilegiando abertos), plano de migração faseada e integração com sistemas existentes; comparação entre simplicidade de um único ecossistema e flexibilidade técnica em multicloud.

3) **Segurança e resiliência (enfoque genérico)**
   - Demonstração de princípios de segurança por defeito e por desenho; encriptação em trânsito e em repouso; controlo de acessos baseado em funções/atributos; registo e auditoria; continuidade de negócio (RPO/RTO e mecanismos de recuperação em cloud).
   - Evidência de proteção de cópias de segurança em repositório logicamente e operacionalmente separado dos ambientes de produção e do DataHub, com imutabilidade e testes periódicos de restauro; conformidade com RGPD e residência de dados na União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia.
   - Comparação do "blast radius" e da separação de identidades nos dois modelos.

4) **Interoperabilidade e integração**
   - Capacidade de integração por APIs, gestão do ciclo de vida das integrações, catálogo/lineage de dados e mecanismos de partilha segura entre plataformas, com avaliação de impactos nos dois modelos.

5) **Operação e governação**
   - Modelos de monitorização/observabilidade, gestão de identidades e acessos, políticas operacionais, runbooks de backup/DR e evidências de testes periódicos; análise da simplificação operacional vs resiliência organizacional em cada modelo.

6) **Vendor lock-in e portabilidade**
   - Identificação de dependências tecnológicas e custos de saída, com estratégias de mitigação (formatos abertos, neutralidade/abstração de dados/serviços), permitindo pesar o risco de aprisionamento tecnológico em ambos os cenários.

4.1 – PLATAFORMA CLOUD CML - CARACTERIZAÇÃO DA CML

4.1.1 - INVENTÁRIO DA INFRAESTRUTURA ON-PREMISES QUE SE PRETENDE MIGRAR PARA A CLOUD CML

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM001	Produção	Microsoft Windows Server 2008 (32-bit)	2	2	34
VM002	Produção	Microsoft Windows Server 2012 (64-bit)	4	8	80
VM003	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	16	100
VM004	Produção	Microsoft Windows Server 2012 (64-bit)	4	4	60
VM005	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	120
VM007	Produção	Microsoft Windows Server 2012 (64-bit)	2	2	60
VM008	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	4	60
VM009	Produção	Microsoft Windows Server 2012 (64-bit)	4	4	40
VM015	Qualidade	Microsoft Windows Server 2012 (64-bit)	4	2	90
VM016	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	80
VM017	Produção	Red Hat Enterprise Linux 4 (32-bit)	4	4	70
VM018	Produção	Microsoft Windows Server 2003 Standard (32-bit)	1	1	16
VM023	Qualidade	Microsoft Windows Server 2003 Standard (32-bit)	2	4	30
VM025	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	40
VM026	Produção	Microsoft Windows NT	1	0,5	64
VM027	Desenvolvimento	Linux CentOS 4/5/6/7 (64-bit)	2	4	80
VM028	Desenvolvimento	Linux CentOS 4/5/6 (64-bit)	2	4	80
VM029	Desenvolvimento	Linux CentOS 4/5/6 (64-bit)	4	16	95
VM030	Desenvolvimento	Linux CentOS 4/5/6 (64-bit)	4	16	95
VM031	Produção	Linux CentOS 7 (64-bit)	4	8	100
VM032	Produção	Linux CentOS 7 (64-bit)	4	16	100
VM033	Qualidade	Oracle Linux	2	16	594
VM034	Produção	Microsoft Windows Server 2003 Standard (32-bit)	2	0,5	105
VM035	Desenvolvimento	Oracle Linux 7 (64-bit)	2	16	594
VM036	Produção	Linux CentOS 7 (64-bit)	4	16	100
VM037	Produção	Linux CentOS 7 (64-bit)	4	16	100

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM038	Produção	Oracle Linux 7 (64-bit)	8	32	594
VM039	Desenvolvimento	Linux CentOS 6 (64-bit)	1	8	410
VM043	Produção	Microsoft Windows Server 2003 (32-bit)	2	1	68
VM044	Qualidade	Red Hat Enterprise Linux 5 (64-bit)	2	16	3334
VM045	Produção	Linux CentOS 6 (64-bit)	4	4	20
VM046	Produção	Microsoft Windows Server 2003 Standard (32-bit)	4	4	45
VM052	Produção	Microsoft Windows Server 2008 R2 (64-bit)	1	6	140
VM053	Qualidade	Microsoft Windows Server 2019 (64-bit)	1	4	60
VM056	Produção	Microsoft Windows Server 2012 (64-bit)	4	4	60
VM058	Produção	Microsoft Windows Server 2008 (64-bit)	2	8	91
VM059	Produção	Microsoft Windows Server 2003 (32-bit)	1	3	50
VM060	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	100
VM061	Desenvolvimento	Microsoft Windows Server 2003 Standard (32-bit)	4	4	100
VM064	Qualidade	Microsoft Windows Server 2003 Standard (32-bit)	2	3	70
VM065	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	60
VM066	Produção	Microsoft Windows Server 2012 (64-bit)	4	6	60
VM067	Produção	Oracle Linux 6 (64-bit)	4	62	1314
VM070	Desenvolvimento	Microsoft Windows Server 2003 Standard (32-bit)	1	4	16
VM071	Produção	Oracle Linux 7 (64-bit)	4	64	712
VM072	Produção	Microsoft Windows Server 2003 Standard (32-bit)	2	4	470
VM073	Qualidade	Microsoft Windows Server 2012 (64-bit)	4	4	1200
VM074	Qualidade	Microsoft Windows Server 2012 (64-bit)	2	4	200
VM075	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	4	60
VM076	Qualidade	Microsoft Windows Server 2012 (64-bit)	1	4	60
VM077	Qualidade	Microsoft Windows Server 2012 (64-bit)	1	4	360
VM081	Qualidade	Microsoft Windows Server 2012 (64-bit)	2	4	60
VM083	Qualidade	Microsoft Windows Server 2012 (64-bit)	2	16	470
VM084	Qualidade	Microsoft Windows Server 2019 (64-bit)	4	6	50

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM085	Qualidade	Microsoft Windows Server 2012 (64-bit)	4	4	71
VM086	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	2	50
VM087	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	2	40
VM088	Qualidade	Microsoft Windows Server 2012 (64-bit)	2	4	60
VM089	Qualidade	Microsoft Windows Server 2012 (64-bit)	2	4	60
VM090	Qualidade	Microsoft Windows Server 2008 R2 (64-bit)	2	4	90
VM091	Qualidade	Microsoft Windows Server 2008 R2 (64-bit)	2	4	60
VM092	Qualidade	Microsoft Windows Server 2012 (64-bit)	4	4	60
VM093	Desenvolvimento	Microsoft Windows Server 2012 (64-bit)	2	2	40
VM094	Qualidade	Microsoft Windows Server 2012 (64-bit)	6	8	950
VM095	Produção	Linux CentOS 4/5 (64-bit)	4	8	60
VM096	Produção	Microsoft Windows Server 2003 Standard (32-bit)	4	4	65
VM097	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	60
VM098	Produção	Microsoft Windows Server 2012 (64-bit)	4	4	160
VM099	Produção	Red Hat Enterprise Linux 5 (64-bit)	4	4	20
VM100	Produção	Microsoft Windows NT	1	1	10
VM102	Produção	Microsoft Windows Server 2003 Standard (32-bit)	4	4	68
VM103	Produção	Microsoft Windows Server 2003 Standard (32-bit)	1	1	15
VM105	Produção	Red Hat Enterprise Linux 6 (64-bit)	4	16	528
VM110	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	60
VM111	Produção	Oracle Linux 7 (64-bit)	4	16	298
VM113	Produção	Other 2.6.x Linux (32-bit)	4	16	180
VM115	Produção	Other Linux (64-bit)	2	6	385
VM117	Produção	Microsoft Windows Server 2008 (32-bit)	2	2	40
VM118	Produção	Linux CentOS 7 (64-bit)	4	2	25
VM124	Produção	Microsoft Windows Server 2012 (64-bit)	2	2	40
VM126	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	60
VM129	Produção	Oracle Linux 7 (64-bit)	4	16	60
VM130	Desenvolvimento	Other 2.6.x Linux (64-bit)	1	2	20

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM131	Qualidade	Oracle Linux 7 (64-bit)	2	8	50
VM132	Qualidade	Oracle Linux 7 (64-bit)	4	16	60
VM139	Produção	Microsoft Windows Server 2012 R2 (64-bit)	4	64	3152
VM140	Produção	Red Hat Enterprise Linux 5 (64-bit)	2	32	1204
VM141	Produção	Microsoft Windows Server 2008 R2 (64-bit)	8	32	608
VM142	Produção	Microsoft Windows Server 2008 (64-bit)	8	32	2161
VM143	Produção	Microsoft Windows Server 2012 (64-bit)	10	32	60
VM145	Produção	Microsoft Windows Server 2019 (64-bit)	4	16	1084
VM147	Desenvolvimento	Oracle Linux 9 (64-bit)	2	16	40
VM148	Desenvolvimento	Oracle Linux 9 (64-bit)	2	2	40
VM149	Desenvolvimento	Oracle Linux 9 (64-bit)	1	4	70
VM150	Desenvolvimento	Oracle Linux 9 (64-bit)	2	16	1064
VM151	Desenvolvimento	Oracle Linux 9 (64-bit)	8	32	1192
VM152	Desenvolvimento	Oracle Linux 9 (64-bit)	2	16	552
VM157	Produção	Oracle Linux 8 (64-bit)	2	6	40
VM159	Produção	Oracle Linux 9 (64-bit)	2	16	40
VM160	Produção	Ubuntu Linux (64-bit)	2	8	60
VM161	Produção	Oracle Linux 9 (64-bit)	8	16	80
VM162	Produção	Oracle Linux 8 (64-bit)	2	4	60
VM163	Produção	Oracle Linux 8 (64-bit)	2	4	60
VM164	Produção	Oracle Linux 9 (64-bit)	2	8	180
VM165	Produção	Oracle Linux 9 (64-bit)	2	8	140
VM166	Produção	Oracle Linux 8 (64-bit)	6	16	60
VM167	Produção	Oracle Linux 8 (64-bit)	4	8	80
VM168	Produção	SUSE Linux Enterprise 12 (64-bit)	4	16	140
VM169	Produção	Other 2.6.x Linux (64-bit)	4	16	504
VM170	Produção	Other 2.6.x Linux (64-bit)	4	16	504
VM171	Produção	Oracle Linux 9 (64-bit)	1	4	80
VM172	Produção	Linux CentOS 7 (64-bit)	4	4	40
VM173	Produção	Oracle Linux 9	2	6	100
VM174	Produção	Linux CentOS 8 (64-bit)	4	8	80
VM175	Produção	Oracle Linux 8 (64-bit)	2	8	190
VM176	Produção	Oracle Linux 9 (64-bit)	2	8	1064
VM177	Produção	Oracle Linux 9 (64-bit)	2	8	140
VM179	Produção	Other Linux (64-bit)	6	8	60
VM180	Produção	Linux CentOS 7 (64-bit)	2	2	40

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM182	Produção	Oracle Linux 8 (64-bit)	4	32	1074
VM183	Produção	Oracle Linux 9 (64-bit)	4	32	3624
VM184	Produção	Oracle Linux 9 (64-bit)	8	64	808
VM185	Produção	Red Hat Enterprise Linux 4	4	32	1702
VM188	Produção	Linux CentOS 7 (64-bit)	8	12	320
VM189	Produção	Oracle Linux 8 (64-bit)	2	2	60
VM190	Produção	Oracle Linux 8 (64-bit)	2	12	200
VM191	Produção	Oracle Linux 8 (64-bit)	4	12	200
VM192	Produção	Oracle Linux 8 (64-bit)	2	8	80
VM193	Produção	Oracle Linux 8 (64-bit)	2	8	80
VM194	Produção	Oracle Linux 9 (64-bit)	2	4	80
VM195	Produção	Rocky Linux (64-bit)	2	8	280
VM196	Produção	Oracle Linux 9 (64-bit)	2	4	60
VM197	Produção	Oracle Linux 8 (64-bit)	8	64	1024
VM198	Produção	Oracle Linux 9 (64-bit)	4	16	3072
VM199	Produção	Oracle Linux 9 (64-bit)	2	16	200
VM201	Produção	Oracle Linux 8 (64-bit)	8	16	140
VM203	Produção	Oracle Linux 9 (64-bit)	1	6	130
VM204	Produção	Oracle Linux 9 (64-bit)	2	4	40
VM208	Produção	Oracle Linux 8 (64-bit)	2	6	60
VM211	Produção	Oracle Linux 9 (64-bit)	2	4	100
VM212	Produção	Linux CentOS 6 (64-bit)	2	4	50
VM213	Produção	Red Hat Enterprise Linux 4 (32-bit)	2	8	163
VM214	Produção	Linux CentOS 6 (64-bit)	2	6	200
VM215	Produção	Debian GNU/Linux 6 (64-bit)	8	8	265
VM216	Produção	Oracle Linux 8 (64-bit)	2	6	30
VM217	Produção	Oracle Linux 8 (64-bit)	2	8	180
VM218	Produção	Oracle Linux 9 (64-bit)	2	6	130
VM219	Produção	Oracle Linux 8 (64-bit)	4	16	300
VM220	Produção	Oracle Linux 8 (64-bit)	2	12	230
VM221	Produção	Oracle Linux 8 (64-bit)	2	8	180
VM222	Produção	Oracle Linux 9 (64-bit)	4	8	100
VM223	Produção	Oracle Linux 9 (64-bit)	2	6	160
VM224	Qualidade	Oracle Linux 8 (64-bit)	2	4	40
VM225	Qualidade	Oracle Linux 9 (64-bit)	2	16	40
VM226	Qualidade	Oracle Linux 9 (64-bit)	2	6	180
VM227	Qualidade	Oracle Linux 9 (64-bit)	2	8	180
VM228	Qualidade	Oracle Linux 8 (64-bit)	2	4	80

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM229	Qualidade	Oracle Linux 9 (64-bit)	1	4	70
VM230	Qualidade	Oracle Linux 9 (64-bit)	1	4	70
VM232	Qualidade	Oracle Linux 9 (64-bit)	2	16	3624
VM233	Qualidade	Oracle Linux 9 (64-bit)	8	32	808
VM234	Qualidade	Oracle Linux 9 (64-bit)	2	16	808
VM235	Qualidade	Rocky Linux (64-bit)	2	4	80
VM236	Qualidade	Oracle Linux 9 (64-bit)	2	4	60
VM237	Qualidade	Oracle Linux 8 (64-bit)	2	4	140
VM239	Qualidade	Oracle Linux 8 (64-bit)	2	6	80
VM241	Qualidade	Oracle Linux 8 (64-bit)	2	6	230
VM243	Qualidade	Oracle Linux 8 (64-bit)	2	8	80
VM244	Qualidade	Oracle Linux 9 (64-bit)	2	4	100
VM245	Desenvolvimento	Oracle Linux 8 (64-bit)	4	16	40
VM247	Produção	Microsoft Windows Server 2016 (64-bit)	16	32	5280
VM248	Qualidade	Microsoft Windows Server 2008 R2 (64-bit)	2	4	80
VM249	Qualidade	Microsoft Windows Server 2008 (64-bit)	12	16	60
VM250	Desenvolvimento	Microsoft Windows Server 2019 (64-bit)	4	16	1560
VM251	Desenvolvimento	Microsoft Windows Server 2019 (64-bit)	2	8	160
VM252	Desenvolvimento	Microsoft Windows Server 2022 (64-bit)	2	6	90
VM253	Desenvolvimento	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM254	Desenvolvimento	Windows Server 2022	2	8	100
VM255	Desenvolvimento	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM256	Desenvolvimento	Windows Server 2022	2	8	100
VM257	Desenvolvimento	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM258	Desenvolvimento	Windows Server 2022	2	8	100
VM259	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	90
VM260	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	90
VM261	Produção	Microsoft Windows Server 2022 (64-bit)	2	16	80
VM263	Produção	Windows Server 2022	2	8	80
VM264	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM266	Produção	Microsoft Windows Server 2016 (64-bit)	8	8	700
VM267	Produção	Microsoft Windows Server 2022 (64-bit)	12	16	140
VM268	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	90

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM269	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	190
VM270	Produção	Microsoft Windows Server 2019 (64-bit)	2	16	160
VM271	Produção	Microsoft Windows Server 2008 (64-bit)	6	16	65
VM272	Produção	Microsoft Windows Server 2003 Standard (32-bit)	2	2	50
VM273	Produção	Microsoft Windows Server 2022 (64-bit)	4	8	100
VM274	Produção	Microsoft Windows Server 2012 (64-bit)	4	16	868
VM275	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM277	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	90
VM279	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	90
VM281	Produção	Windows Server 2019	2	8	60
VM286	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	90
VM287	Produção	Microsoft Windows Server 2022 (64-bit)	2	4	90
VM288	Produção	Microsoft Windows 10 (32-bit)	4	3,5	41
VM289	Produção	Microsoft Windows 10 (32-bit)	4	3,5	41
VM290	Produção	Microsoft Windows 10 (32-bit)	4	3,5	41
VM291	Produção	Microsoft Windows Server 2003 (32-bit)	4	4	136
VM292	Produção	Microsoft Windows Server 2022 (64-bit)	4	8	90
VM293	Produção	Microsoft Windows Server 2022 (64-bit)	4	8	90
VM294	Produção	Microsoft Windows Server 2019 (64-bit)	6	16	160
VM295	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	150
VM296	Produção	Microsoft Windows Server 2019 (64-bit)	16	128	4668
VM297	Produção	Microsoft Windows Server 2019 (64-bit)	8	32	180
VM298	Produção	Microsoft Windows 10 (64-bit)	6	16	60
VM299	Produção	Microsoft Windows 10 (64-bit)	6	16	60
VM300	Produção	Microsoft Windows 10 (64-bit)	6	16	60
VM301	Produção	Microsoft Windows 10 (64-bit)	6	12	60
VM302	Produção	Microsoft Windows 10 (64-bit)	6	12	60
VM303	Produção	Microsoft Windows 10 (64-bit)	6	12	60
VM304	Produção	Microsoft Windows Server 2012 (64-bit)	4	8	60

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM305	Produção	Microsoft Windows XP Professional (32-bit)	4	3	98
VM308	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM309	Produção	Microsoft Windows XP Professional (32-bit)	1	4	92
VM310	Produção	Microsoft Windows Server 2019 (64-bit)	4	8	60
VM311	Produção	Microsoft Windows 10 (64-bit)	4	16	120
VM312	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM313	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM314	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM315	Produção	Microsoft Windows 10 (64-bit)	2	6	70
VM316	Produção	Microsoft Windows 10 (64-bit)	2	16	60
VM317	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM318	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM319	Produção	Microsoft Windows 10 (64-bit)	2	6	80
VM320	Produção	Microsoft Windows 10 (64-bit)	2	16	100
VM321	Produção	Microsoft Windows 11 (64-bit)	2	8	90
VM322	Produção	Microsoft Windows 11 (64-bit)	2	8	100
VM323	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM324	Produção	Microsoft Windows 11 (64-bit)	2	16	100
VM325	Produção	Microsoft Windows 11 (64-bit)	4	16	80
VM326	Produção	Microsoft Windows 11 (64-bit)	4	16	80
VM327	Produção	Microsoft Windows 11 (64-bit)	2	8	60
VM328	Produção	Microsoft Windows 11 (64-bit)	2	8	120
VM329	Produção	Microsoft Windows 11 (64-bit)	2	8	60
VM330	Produção	Microsoft Windows 11 (64-bit)	2	16	60
VM331	Produção	Microsoft Windows 11 (64-bit)	2	8	60
VM332	Produção	Microsoft Windows 11 (64-bit)	2	8	80
VM333	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM334	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	60
VM335	Produção	Microsoft Windows Server 2016 (64-bit)	8	128	2136

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM336	Produção	Microsoft Windows Server 2012 (64-bit)	4	16	80
VM339	Produção	Microsoft Windows Server 2022 (64-bit)	4	8	90
VM341	Produção	Microsoft Windows Server 2019 (64-bit)	4	8	60
VM342	Produção	Microsoft Windows Server 2012 (64-bit)	6	6	1102
VM343	Produção	Microsoft Windows Server 2012 (64-bit)	4	4	190
VM344	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM345	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM346	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM347	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	80
VM351	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM352	Produção	Microsoft Windows Server 2019 (64-bit)	2	4	90
VM353	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM356	Produção	Microsoft Windows Server 2012 (64-bit)	4	6	296
VM357	Produção	Microsoft Windows Server 2012 (64-bit)	6	10	120
VM358	Produção	Microsoft Windows 10 (64-bit)	4	8	90
VM362	Produção	Microsoft Windows Server 2022 (64-bit)	4	8	130
VM367	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	120
VM369	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM370	Produção	Microsoft Windows Server 2022 (64-bit)	4	16	
VM371	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM372	Produção	Microsoft Windows Server 2022 (64-bit)	4	16	
VM373	Produção	Windows Server 2025	4	16	
VM374	Produção	Windows Server 2025	4	16	
VM375	Produção	Windows Server 2025	4	16	
VM376	Produção	Windows Server 2025	4	16	
VM377	Produção	Windows Server 2025	4	16	
VM379	Produção	Microsoft Windows Server 2022 (64-bit)	4	32	80
VM381	Produção	Microsoft Windows 10 (64-bit)	2	6	60
VM382	Produção	Microsoft Windows 7 (32-bit)	4	8	40
VM383	Produção	Microsoft Windows 7 (32-bit)	4	8	40

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM385	Produção	Microsoft Windows 10 (64-bit)	4	32	120
VM386	Produção	Microsoft Windows 10 (64-bit)	4	32	120
VM388	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM389	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	120
VM390	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	40
VM392	Produção	Microsoft Windows Server 2019 (64-bit)	2	8	60
VM393	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	60
VM394	Produção	Microsoft Windows Server 2012 (64-bit)	2	4	40
VM395	Produção	Microsoft Windows Server 2019 (64-bit)	6	12	155
VM396	Produção	Microsoft Windows Server 2022 (64-bit)	4	8	130
VM398	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	8	190
VM399	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	8	160
VM400	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	8	160
VM401	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	8	150
VM402	Qualidade	Microsoft Windows Server 2019 (64-bit)	4	16	3060
VM403	Qualidade	Microsoft Windows Server 2019 (64-bit)	4	8	160
VM405	Qualidade	Windows Server 2022	2	8	180
VM407	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	8	280
VM408	Qualidade	Microsoft Windows Server 2022 (64-bit)	4	12	160
VM409	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	8	280
VM410	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	12	160
VM411	Qualidade	Microsoft Windows Server 2022 (64-bit)	4	8	90
VM412	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	8	180
VM413	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	8	80
VM414	Qualidade	Microsoft Windows Server 2022 (64-bit)	2	8	100
VM415	Qualidade	Windows Server 2025	2	8	120
VM416	Qualidade	Microsoft Windows Server 2022 (64-bit)	16	16	250
VM417	Qualidade	Microsoft Windows Server 2022 (64-bit)	16	16	250
VM418	Qualidade	Microsoft Windows Server 2022 (64-bit)	16	16	150
VM419	Qualidade	Microsoft Windows Server 2022 (64-bit)	16	16	150

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM420	Qualidade	Microsoft Windows Server 2022 (64-bit)	16	16	250
VM421	Qualidade	Microsoft Windows Server 2022 (64-bit)	16	16	250
VM422	Qualidade	Windows Server 2025	2	8	330
VM423	Qualidade	Windows Server 2025	2	8	300
VM424	Qualidade	Windows Server 2022	2	8	100
VM425	Qualidade	Microsoft Windows Server 2019 (64-bit)	2	8	120
VM426	Qualidade	Linux CentOS 7 (64-bit)	2	2	40
VM427	Desenvolvimento	Red Hat Enterprise Linux 4 (32-bit)	4	12	691
VM428	Produção	Oracle Linux 7 (64-bit)	2	32	1 180
VM429	Desenvolvimento	Oracle Linux 7 (64-bit)	1	16	748
VM430	Qualidade	Oracle Linux 7 (64-bit)	2	8	664
VM431	Produção	Oracle Linux 7 (64-bit)	10	64	796
VM433	Produção	Oracle Linux 6 (64-bit)	2	32	684
VM434	Desenvolvimento	Oracle Linux 7 (64-bit)	1	16	1 160
VM435	Qualidade	Oracle Linux 7 (64-bit)	2	16	856
VM436	Desenvolvimento	Oracle Linux 6 (64-bit)	2	16	786
VM437	Produção	Oracle Linux 6 (64-bit)	8	16	126
VM438	Desenvolvimento	Oracle Linux 6 (64-bit)	4	16	80
VM439	Qualidade	Oracle Linux 6 (64-bit)	2	16	126
host001	Produção	Red Hat Enterprise Linux Server release 5.8 (Tikanga)	8	28	6092
host003	Produção	Windows Server 2012 R2	16	256	10250

- Total de máquinas = 329
- Total de vCPU = 1132
- GB de Memória = 111255
- TB de storage = 108,7 TB

4.1.2 - INVENTÁRIO DA INFRAESTRUTURA ON-PREMISES QUE DEVERÁ TER DISASTER RECOVERY

A - SISTEMAS LIGADOS À SEGURANÇA, EMERGÊNCIA

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VM006	Produção	Linux CentOS 4/5 (64-bit)	2	2	16
VM019	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	40
VM020	Produção	Microsoft Windows Server 2012 (64-bit)	4	64	60
VM021	Produção	Microsoft Windows Server 2012 (64-bit)	2	2	60
VM022	Produção	Microsoft Windows Server 2003 Standard (64-bit)	2	4	137
VM057	Produção	Linux CentOS 4/5 (64-bit)	4	4	50
VM104	Produção	Microsoft Windows Server 2012 (64-bit)	2	2	120
VM119	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	40
VM120	Produção	Microsoft Windows Server 2012 (64-bit)	2	8	40
VM122	Produção	Microsoft Windows Server 2012 (64-bit)	1	4	60
VM134	Produção	Oracle Linux 4/5 (64-bit)	2	8	50
VM158	Produção	Linux CentOS 4/5 (64-bit)	4	8	20
VM186	Produção	Oracle Linux 9 (64-bit)	4	32	808
VM202	Produção	Oracle Linux 8 (64-bit)	1	2	50
VM306	Produção	Microsoft Windows Server 2019 (64-bit)	4	32	290
VM307	Produção	Microsoft Windows Server 2019 (64-bit)	4	32	290
VM359	Produção	Microsoft Windows Server 2022 (64-bit)	4	16	220
VM360	Produção	Microsoft Windows Server 2022 (64-bit)	4	12	300
VM361	Produção	Microsoft Windows Server 2022 (64-bit)	2	12	200
VM363	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	200
VM364	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	150
VM365	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	120
VM366	Produção	Microsoft Windows Server 2022 (64-bit)	2	8	160
VM432	Produção	Red Hat Enterprise Linux 4 (32-bit)	2	6	58
VM447	Produção	AIX 7.1 7100-05-02-1832	8	32	1920
VM454	Produção	AIX 7.1 7100-05-02-1832	12	128	16000
VM456	Produção	AIX 7.2 7200-03-01-1838	8	32	740
VM467	Produção	AIX 7.2 7200-03-01-1838	1	8	390
host002	Produção	Red Hat Enterprise Linux AS release 4 (Nahant Update 5), 32 bits	8	36	3160

- Total de máquinas = 29
- Total de vCPU = 99
- GB de Memória = 534
- TB de storage = 25,15 TB

B - SISTEMAS DE SUPORTE À PLATAFORMA DE GESTÃO INTELIGENTE DE LISBOA (PGIL)

Tipologia	Ambiente	SO + Versão	CPU (Cores)	Memória (GB)	Storage (GB total)
VMPGIL01	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	100
VMPGIL02	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	100
VMPGIL03	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	100
VMPGIL04	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	100
VMPGIL05	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	100
VMPGIL06	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	3 122
VMPGIL07	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	80
VMPGIL08	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	48	250
VMPGIL09	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	48	250
VMPGIL10	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	48	250
VMPGIL11	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	48	350
VMPGIL12	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	48	350
VMPGIL13	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	48	350
VMPGIL14	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	64	850
VMPGIL15	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	64	850
VMPGIL16	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	64	850
VMPGIL17	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	64	850
VMPGIL18	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	32	1 586
VMPGIL19	Produção	Ubuntu Linux 22.04 LTS (64-bit)	16	32	182
VMPGIL20	Produção	Ubuntu Linux 22.04 LTS (64-bit)	4	8	50
VMPGIL21	Produção	Microsoft Windows Server 2012 (64-bit)	8	8	100
VMPGIL22	Produção	Oracle Linux 8 (64-bit)	8	8	240
VMPGIL23	Produção	CentOS 7 (64-bit)	8	16	8 392

- Total de máquinas = 23
- Total de vCPU = 248
- GB de Memória = 704
- TB de storage = 19 TB

4.1.3 - ORIENTAÇÃO DE MIGRAÇÃO, RESILIÊNCIA E SERVIÇOS CONTRATADOS

A prioridade da CML é realizar uma MIGRAÇÃO RÁPIDA (CUTOVER) para a cloud, ativando o serviço de Cloud Backup desde o “Day-0”. A modernização e otimização das aplicações decorre já em cloud (sem faseamento prévio da migração). Não se exigem serviços de alta

disponibilidade (HA) para workloads em cloud, exceto no caso do DR em cloud que cobre apenas os sistemas críticos on-premises ligados à segurança/emergência e aos sistemas de suporte à Plataforma de Gestão Inteligente de Lisboa; pretende-se proteção robusta dos dados (backup segregado, imutável e testado) e SLAs de reposição alinhados com práticas da administração pública.

Os serviços a contratar abrangem a implementação e operação por 4 anos da Plataforma Cloud CML e do Data Recovery em cloud para sistemas on-premises críticos, incluindo: migração, modernização, backup/recuperação, segurança, monitorização, suporte, formação e transferência de conhecimento, consultoria e gestão financeira (FinOps), com residência de dados na EU, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia e conformidade RGPD/NIS2/ISO.

4.1.4 — REQUISITOS FUNCIONAIS (O QUE A CML PRETENDE OBTER)

F1. Migração rápida (bulk cutover) com mínima indisponibilidade

- Mover, em bloco, aplicações e dados do on-premises para cloud, preservando configurações e validando integridade pós-migração.

F2. Cloud Backup operacional "Day-0"

- Backup/restore ativo desde o arranque em cloud, com repositório de backup logicamente e operacionalmente separado do ambiente de produção, testes periódicos de restauro e evidências de integridade/encriptação.

F3. Continuidade sem Alta Disponibilidade (HA – *High Availability)* para workloads em cloud (via backup/restauro)

- Definir objetivos orientativos de continuidade: RPO ≤ 24h e RTO ≤ 24h (ajustáveis por classe de aplicação), aceitando janelas de reposição por via de restauro.

F4. Modernização e otimização já em cloud

- Suporte a refactor/re-platform com serviços nativos (ex.: contentores/orquestração, auto-scaling, balanceamento, storage otimizado) para ganhos de performance e custo.

F5. Conectividade e integração híbrida

- Conectividade segura cloud ⇄ Data Center/Redes CML; interoperabilidade com sistemas existentes e integração com o Lisboa DataHub.

F6. Identidades, acessos e governação

- IAM centralizado, least-privilege e segregação de funções; etiquetagem (tags) para governação, custeio e conformidade.

F7. Observabilidade e alertas

- Monitorização unificada de desempenho, utilização e segurança, com dashboards e alertas tendencialmente em tempo real.

F8. Conformidade e proteção de dados

- Alinhamento com RGPD/NIS2 e políticas internas CML; residência de dados e backups em regiões da União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia; suporte a auditoria.

F9. Suporte e transferência de conhecimento

- Suporte graduado (reforçado nos primeiros 12 meses), formação e transferência de conhecimento contínua para equipas CML.

4.1.5 — REQUISITOS TÉCNICOS (PARÂMETROS, CONTROLOS E MEDIÇÕES)

T1. Landing zone pronta (Day-0)

- Guardrails/políticas, redes, KMS/chaves, logging/auditoria, etiquetagem obrigatória e integração com identidade corporativa.

T2. Ferramentas/métodos de migração em bloco

- Migração de VMs, bases de dados e ficheiros (agentless/agent-based, online/offline), com aceleração e validação pós-migração (checksums, testes funcionais).

T3. Backup segregado e proteção de dados

- Backups automáticos, pelo menos diários; retenção ≥ 30 dias.
- Repositório de backup em infraestrutura distinta (conta/subscrição/tenant ou serviço dedicado), com imutabilidade (WORM) e residência na União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia.
- Encriptação em repouso (ex.: AES-256 ou equivalente) e em trânsito (ex.: TLS 1.2+).
- Relatórios automáticos de execução/integridade; testes periódicos de restauro documentados.

T4. RPO/RTO de workloads em cloud (sem HA)

- RPO orientativo ≤ 24h; RTO orientativo ≤ 24h (por classe de aplicação).
- Runbooks de restauro validados; evidências de testes e tempos práticos de reposição.

T5. Redes e interconexão

- VPNs e/ou interconexões dedicadas; segmentação, firewalls e micro-segmentação.
- Latências: apresentar latências típicas por região/opção e mitigação em integrações críticas (objetivo indicativo ≤ 10 ms).

T6. Segurança por defeito (Zero Trust)

- MFA; IAM com SoD; hardening; gestão de vulnerabilidades; registos/auditoria integrados; retenção de logs conforme normativos legais e em vigor na CML.

T7. Contentores e orquestração

- Execução/gestão de contentores com serviço gerido de Kubernetes (ou equivalente), políticas de segurança (ex.: Pod Security/OPA), registo de imagens e atualizações.

T8. Observabilidade e registos

- Telemetria (métricas, logs, traces) centralizada; dashboards/alertas configuráveis; integração com SIEM/SOC (quando aplicável).

T9. Conformidade e certificações

- Evidências/certificações alinhadas com ISO/IEC 27001, 27017, 27018 (ou equivalentes), RGPD e NIS2; documentação para auditorias.

T10. Controlo de custos (FinOps)

- Ferramentas de previsão/otimização, orçamentação, alertas de consumo, recomendações; etiquetagem obrigatória para chargeback/showback.

T11. Integração CI/CD e automação

- Integração com pipelines CI/CD, infra-as-code, testes e blue/green/canary; controlos de segurança (DevSecOps).

T12. Reversibilidade (exit) e portabilidade

- Exportação de dados/artefactos em formatos abertos; plano de reversibilidade (tempos,

passos, custos) para migração intra/inter-cloud ou retorno on-premises.

4.1.6 — DATA RECOVERY (DR) EM CLOUD — SISTEMAS CRÍTICOS ON-PREMISES (APLICAÇÕES DE SEGURANÇA/EMERGÊNCIA) E AOS SISTEMAS DE SUPORTE À PLATAFORMA DE GESTÃO INTELIGENTE DE LISBOA

(Aplica-se apenas a cargas que permanecem on-premises.)

A) Funcionais

DR1. Replicação/sincronização para cloud de componentes críticos (ver 4.1.2 A e B).

DR2. Ativação (failover) em cloud por sistema/total/parcial consoante indisponibilidades no Data Center da CML.

DR3. Manutenção de configurações/dados necessários à continuidade operacional nos recursos ativados em cloud.

DR4. Testes semestrais ao processo de recuperação/failover com registo de evidências.

B) Técnicos

DR5. Replicação contínua ou periódica com relatórios automáticos de sincronização e testes.

DR6. Compatibilidade com OS/aplicações existentes no Data Center.

DR7. RTO (ativação de recursos em cloud) ≤ 4 horas.

DR8. Encriptação em trânsito e em repouso em todo o processo.

DR9. Conformidade com ISO/IEC 27001, 27017, 27018 e RGPD; residência na União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia.

4.1.7 — SERVIÇOS A PRESTAR (IMPLEMENTAÇÃO + OPERAÇÃO 4 ANOS)

O contrato deve abranger serviços integrados para a Plataforma Cloud CML e DR em cloud dos sistemas on-premises críticos, garantindo residência EU, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia e conformidade RGPD/NIS2/ISO:

a) Serviços cloud (requisitos gerais)

- Compatibilidade multi-OS (ex.: Windows/Linux); segurança avançada (encriptação, firewalls, IAM, MFA); conformidade ISO 27001/27017/27018, RGPD, NIS2.
- Objetivo de disponibilidade do ambiente cloud: ≥ 99,5% (orientativo); sem exigência de HA aplicacional em cloud.

b) Serviços de migração e modernização

- Inventário (ver 4.1.1), migração bulk lift-and-shift (janela por VM objetivo ≤ 2h), conclusão sem perda de dados; relatórios de performance pós-migração; modernização cloud-native (contentores/orquestração, CI/CD).
- Objetivo durante janelas de migração: minimizar indisponibilidade, com plano de cutover e comunicação.

c) Serviços de Cloud Backup (workloads em cloud)

- Backup automatizado (mínimo diário) com retenção ≥ 30 dias; testes de restauração completos; encriptação AES-256/TLS ≥ 1.2; armazenamento das cópias em infraestrutura distinta na União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia.
- Resolução de falhas de jobs de backup: ≤ 4h (objetivo).
- RPO/RTO orientativos de reposição por restauro: RPO ≤ 24h; RTO ≤ 24h (por classe).

d) Serviços de Data Recovery em cloud (apenas sistemas críticos on-premises)

- Replicação contínua, failover orquestrado, runbooks e testes semestrais; encriptação AES-256/TLS ≥ 1.2.
- RTO para ativação de recursos críticos: ≤ 4h.
- Objetivo de disponibilidade da capacidade de DR: ≥ 99,9%.

e) Serviços de segurança e Gestão de Identidade e Acesso [Identity and Access Management (IAM)]

- IAM centralizado (RBAC/ABAC, MFA, SoD, auditoria); firewalls, segmentação e VPN; monitorização de segurança com alertas/dashboards; testes de penetração (periodicidade a acordar).

f) Serviços de monitorização e suporte

- Monitorização 24/7 (desempenho, segurança, custos); relatórios mensais no 1.º ano e

trimestrais nos seguintes; alertas em tempo real; suporte reforçado no 1.º ano e suporte nos anos seguintes.

- SLA de resposta inicial a incidentes: ≤ 4h (orientativo).

g) Serviços de formação e transferência de conhecimento

- Plano de capacitação contínuo e transferência de conhecimento para técnicos CML, abrangendo administração, operações, segurança, FinOps, práticas DevOps/DataOps, gestão de identidades, governança de dados, monitorização e ferramentas específicas da plataforma cloud.

h) Serviços de consultoria (operação e melhoria contínua)

- Apoio à gestão, FinOps e operação da Cloud CML, incluindo planeamento e execução de melhorias contínuas, suporte à integração com sistemas existentes e novos, otimização de custos e recursos, monitorização de desempenho, gestão de identidades e segurança, e alinhamento com práticas de governança e compliance.

i) Serviços de FinOps & conformidade

- Ferramentas FinOps para previsão/otimização/alertas; relatórios de custos e utilização; dashboards ativos; checklists RGPD/NIS2/ISO com evidências de conformidade/certificações.

j) Licenciamento (no aplicável)

i. Windows Server

- Versões suportadas: Identificar versões compatíveis com o ambiente cloud.
- Modelos de licenciamento:
  - SPLA (Service Provider License Agreement).
  - BYOL (Bring Your Own License).
  - Subscrição nativa em cloud.
- Integração com Active Directory (AD): Garantir compatibilidade com serviços de identidade híbridos.

ii. Base de Dados Oracle

- Instâncias on-premises migradas para IaaS ou PaaS.
- Opções em cloud: Avaliar serviços geridos vs infraestrutura dedicada.
- Conformidade contratual: Garantir aderência às políticas Oracle.
- Otimização de custos: Considerar licenciamento por núcleo, métricas de consumo e possíveis descontos.

iii. Proteção de Endpoint

- Soluções integradas: Equivalentes a Microsoft Defender ou Trend Micro.
- Cobertura: Máquinas virtuais, contentores e workloads híbridos.
- Modelo de subscrição: Custos por instância ou por utilizador.

iV. Firewalls Avançadas

- Serviços nativos do fornecedor cloud (equivalentes a firewalls de próxima geração).
- Funcionalidades:
- Segmentação de rede.
    - Inspeção L7.
    - Integração com SIEM.
    - Custos: Subscrição mensal ou por throughput.

V. Virtualização

- Avaliação estratégica:
    - Manutenção de VMware (com custos de licenciamento e suporte).
    - Alternativa: Cotação para licenciamento adicional de máquinas Legacy de versões não suportada pela virtualização proprietária nativa do fornecedor (ex. VMWare).
- Critérios: Compatibilidade, custo total de propriedade (TCO) e suporte técnico.

A cotação relativa a licenciamento a favor da CML, será exclusivamente sobre o necessário e deve ser apresentada por tipo de licenciamento e separada, cabendo à CML a decisão sobre a sua aquisição.

k) Documentação e relatórios

- Relatórios mensais no 1.º ano e trimestrais nos seguintes (desempenho, segurança, custos); evidências de testes de backup/DR; documentação de conformidade/auditoria.

Notas finais:

— HA só se aplica aos sistemas críticos que permanecem on-premises e têm DR em cloud (secção 4.1.6).
— Para workloads em cloud, a continuidade faz-se por backup/restauro com RPO/RTO orientativos e SLAs de suporte razoáveis, para evitar custos excessivos.
— Downtime máximo de 0,01% por ano.
— As referências tecnológicas são exemplos; admitem-se equivalentes funcionais.
— SLAs detalhados, métricas/penalizações e matrizes de responsabilidade serão especificados em capítulo próprio; esta secção estabelece linha funcional/técnica e de

serviços para comparação de propostas.

— A proposta deve acautelar a escalabilidade na proporção de 15% por ano, e a partir do 1º ano de contrato (CPU, memória e storage).
— Assegurar o funcionamento de servidores com 32 bits e sistemas operativos legacy sem suporte.
— Garantir o mesmo endereçamento IP (existem aplicações com os IP's no código).
— Disponibilização de ferramentas (Data Pump, RMAN e GoldenGate).

4.2 - PLATAFORMA LISBOA DATAHUB

A Câmara Municipal de Lisboa pretende criar, em cloud, uma plataforma central de dados — Lisboa DataHub — com os seguintes objetivos:

1) Integrar dados de múltiplas fontes

- Reunir, num único ponto, informação proveniente de sistemas internos e soluções SaaS, permitindo troca e reutilização de dados de forma segura e controlada. Deve garantir orquestração e interoperabilidade com o mínimo de esforço, através de conectores universais, APIs abertas, motor de workflows, suporte a formatos e protocolos padrão, gestão centralizada, segurança robusta e catálogo de dados para governança.

2) Assegurar governação e qualidade

- Aplicar regras claras de qualidade, privacidade e acesso, com registo/auditoria, para que os dados sejam confiáveis, consistentes e utilizáveis pelas equipas da CML.

3) Catalogar e tornar os dados descobríveis

- Disponibilizar um catálogo com metadados e "linha de vida" dos conjuntos de dados (origem → transformação → uso), facilitando a descoberta e o reaproveitamento.

4) Disponibilizar dados para consumo interno e externo

- Criar: um Portal Interno de Dados para serviços municipais (self-service, analítica e relatórios),
- E suportar o Portal de Dados Abertos, garantindo proteção de dados pessoais e conformidade legal.

5) Promover analítica e inteligência

- Fornecer condições para dashboards, relatórios e modelos analíticos/IA governados, que apoiem decisões baseadas em evidência e inovação em serviços públicos.

6) Operar com segurança e conformidade

- Garantir segurança por defeito e por desenho (RGPD/NIS2), com residência de dados na União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia, e controlo de acessos adequado às políticas da CML.

7) Assegurar continuidade por via de backup (sem alta disponibilidade)

- Proteger os dados do DataHub com cópias de segurança automatizadas, guardadas de forma segregada, encriptadas e testadas regularmente, para reposição em caso de incidente — não é requerida alta disponibilidade para o DataHub.

8) Controlar custos e evitar dependências

- Adotar práticas de gestão financeira (FinOps) e privilegiar formatos abertos/interoperáveis, mitigando riscos de dependência excessiva de fornecedor.

Com o Lisboa DataHub, a CML obtém uma base fiável para partilha e exploração de dados, reforça a transparência e a eficiência, e acelera a criação de valor (analítica e IA) em benefício dos cidadãos e da gestão municipal.

Face aos atuais desafios e objetivos identificados a implementação da plataforma Lisboa DataHub terá de ser faseada, abrangendo a migração de dados provenientes de soluções SaaS, como sejam de sistemas ERP, de gestão de ativos, stocks e operações, de gestão de contratos públicos ou outros, bem como da informação/dados atualmente alojada em servidores no Data Center da CML e/ou em cloud. O quadro seguinte apresenta uma caracterização resumo para as três tecnologias de base de dados mais utilizadas na CML, a saber: MSSQL, POSTGRESQL e ORACLE.

Quadro-síntese para referência de dados para quantificação do DataHub:

Tecnologia	Volume Total BD (GB)	Nº Servidores Distintos	Volume Total Filesystem (GB)
MSSQL	3070,9	6	2483
ORACLE	9850,9	16	8528
POSTGRESQL	617,9	3	735

4.2.1 REQUISITOS FUNCIONAIS — O QUE A CML PRETENDE OBTER COM O LISBOA DATAHUB

F1. Integração de múltiplas fontes de dados

- Integrar, numa plataforma única, dados provenientes do Data Center municipal, clouds externas e aplicações SaaS, cobrindo formatos estruturados, semi-estruturados e não estruturados.

F2. Acesso unificado e descoberta de dados

- Disponibilizar datasets validados através de mecanismos de self-service ou subscrição; oferecer uma interface intuitiva para pesquisa, navegação e consumo de dados por perfis técnicos e de negócio.

F3. Desempenho adequado ao uso (dois perfis de serviço)

- APIs Operacionais (baixa latência): para usos transacionais e preenchimento de campos em tempo quase real (objetivos indicativos de milissegundos, quando tecnicamente viável).
- APIs de Exploração (latência superior): para análises e consultas complexas, tolerando segundos/minutos de latência em benefício de abrangência e custo.

F4. Qualidade, ciclo de vida e governação

- Aplicar regras de qualidade na ingestão e transformação (perfilagem, validação, limpeza); gerir metadados e rastrear o ciclo de vida (lineage) dos dados; monitorizar continuamente a qualidade e conformidade.

F5. Segurança e conformidade por defeito e por desenho

- Implementar RBAC/ABAC (controlo por funções/atributos, inclusive por colunas/linhas), segregação de funções, auditoria e monitorização de uso; assegurar privacidade e conformidade com RGPD/NIS2.

F6. Catálogo central e inventário de APIs

- Disponibilizar catálogo para pesquisa de datasets, metadados e lineage; manter inventário de APIs com documentação de uso e políticas de partilha segura.

F7. Continuidade sem HA (por via de backup/restauro)

- Proteger os dados do DataHub com cópias de segurança automatizadas para infraestrutura distinta da principal (lógica/operacionalmente separada), encriptadas, com verificação de integridade e testes regulares de recuperação (sem exigência de alta disponibilidade).

F8. Valor para a decisão e inovação

- Suportar BI, analítica e uso responsável de IA; disponibilizar dados para consumo interno (Portal Interno de Dados) e para dados abertos (com anonimização/pseudonimização quando aplicável).

4.2.2 REQUISITOS TÉCNICOS — PARÂMETROS, CONTROLOS E PORTABILIDADE

T1. Escalabilidade e elasticidade

- Escalar automaticamente com base em volume/consumo; privilegiar serviços *serverless quando adequado (eficiência de custos e operação); definir SLOs de desempenho e configurar alertas/observabilidade.

T2. Observabilidade e operação

- Centralizar logs, métricas e traces; painéis e alarmística para pipelines, APIs e consumo; retenção e políticas de registos em linha com normativos CML e legais.

T3. Mitigação de vendor lock-in e plano de saída

- Formatos abertos: JSON, CSV, Parquet (e afins).
- APIs padrão: REST/GraphQL com documentação aberta.
- Arquitetura portável: contentores e orquestração (ex.: Kubernetes ou equivalente).
- IaC multicloud: Terraform (ou equivalente) para landing zones e serviços.
- Lógica desacoplada: separar regra de negócio da infraestrutura/serviços específicos.
- Portabilidade de dados: exportação regular com metadados e estrutura preservados; plano de reversibilidade documentado.

T4. Segurança por defeito

- Encriptação em repouso (ex.: AES-256 ou equivalente) e em trânsito (ex.: TLS 1.2+); IAM centralizado, MFA, segregação de funções, gestão de vulnerabilidades e hardening; auditoria e prestação de contas.

T5. Ingestão batch e stream

- Ingerir dados por lotes e eventos/fluxos; suportar dados alfanuméricos, georreferenciados, imagem, áudio e vídeo; integrar com SGBDs existentes (ex.: SQL Server, Oracle, PostgreSQL), garantindo compatibilidade e sem perda de funcionalidades.

T6. Lakehouse/Modelo de dados

- Estruturar raw e curated; definir regras de negócio, agregações, reference/master data; materializar datasets com latências ajustadas ao perfil (operacional vs exploratório); suportar semântica/modelação.

T7. Catálogo e governação descentralizada

- Permitir governação por temas/subtemas; suportar metadados e lineage a montante e

jusante; rastrear dados para RGPD (ex.: direito ao apagamento); publicar métricas de qualidade dos dados.

T8. Exploração e interoperabilidade

- Ferramentas de pesquisa/descoberta; suporte a SQL (não exclusivo) e virtualização de dados; armazenamento/partilha de views; ligação nativa a ferramentas BI (ex.: Power BI) e integração com ambientes de IA governados.

T9. Gestão de APIs (API Management)

- Inventariar, proteger e versionar APIs; gerir subscrições e limites; IAM aplicado a modos público/restrito; métricas de uso/desempenho e alarmística de consumo; exposição do lineage associado a APIs.

T10. Backup do DataHub (continuidades)

- Backup automatizado, frequência mínima diária; retenção ≥ 30 dias.
- Repositório de backup em infraestrutura distinta (conta/subscrição/tenant ou serviço dedicado) com imutabilidade (WORM) e residência na União Europeia, garantindo a não existência de fluxos transfronteiriços para fora da União Europeia.
- Encriptação em trânsito e em repouso; verificação de integridade (checksums).
- Testes periódicos de recuperação documentados.
- Objetivos orientativos: RPO ≤ 24h; RTO ≤ 24h (sem HA).
- (HA não é requerido para o DataHub; a continuidade faz-se por backup/restauro.)

T11. Conformidade

- Evidências/certificações alinhadas com ISO/IEC 27001, 27017, 27018 (ou equivalentes), RGPD e NIS2; documentação para auditorias e due-diligence.

4.2.3 SERVIÇOS A PRESTAR — IMPLEMENTAÇÃO, OPERAÇÃO EFICIENTE E TRANSFERÊNCIA DE CONHECIMENTO

S1. Implementação e landing do DataHub

- Apoio na implementação de landing zones, identidade, políticas/guardrails, redes, observabilidade e segurança; configuração inicial de ingestão, catálogo e API Management; plano de dados (domínios prioritários).

S2. Migração de dados e modernização

- Produção de inventário de fontes, plano de transformação/carga; adoção de práticas data reliability e data quality; melhoria contínua de pipelines (reprocessamento e rollback controlado).

S3. Operação e suporte (4 anos)

- Operação 24/7 do DataHub (pipelines, APIs, catálogo), observabilidade e gestão de incidentes; SLAs razoáveis de resposta/mitigação em linha com práticas da AP; runbooks; relatórios mensais (desempenho, segurança, custos).

S4. Segurança e conformidade

- Gestão de IAM, políticas de acesso, auditoria, testes de privacidade e privacy by design; evidências RGPD/NIS2/ISO; revisão periódica de controlos.

S5. Backup e testes de recuperação

- Execução de jobs de backup, verificação de integridade e testes de restauro; relatórios com evidências de encriptação e tempos de recuperação.

S6. FinOps e otimização contínua

- Ferramentas/processos de previsão e otimização de custos; tagging obrigatório; showback/chargeback; recomendações de rightsizing e desenho eficiente.

S7. Formação e transferência de conhecimento

- Plano de capacitação por perfis (básico/analista/avançado), sessões práticas e documentação; shadowing e handover operacionais; objetivo de autonomizar gradualmente a equipa técnica da CML.

S8. Documentação e entregáveis

- Arquitetura implementada e operacional; documentação técnica/funcional; planos de operação, formação e transferência de conhecimento; relatórios periódicos (serviço, qualidade, custos e conformidade).

5. INFORMAÇÃO PRETENDIDA

De seguida são apresentadas algumas orientações gerais para que, voluntariamente, os operadores económicos nos disponibilizem informação em resposta a esta Consulta Preliminar.

A informação disponibilizada deverá ter em conta os modelos referidos no ponto 4 deste documento.

Sempre que aplicável, devem ser apresentadas soluções para os modelos A e B. Caso um modelo não seja aplicável, justificar de forma objetiva.

5.1. GUIÃO DE APRESENTAÇÃO DA SOLUÇÃO PARA CADA MODELO A / B

- **Arquitetura (alto nível): [diagramas/descrição breve], detalhando por componente:**
  - CLOUD CML
    - Landing zone, redes, IAM, políticas/guardrails, observabilidade: [descrição]
    - Migração cutover (método, janelas por VM, validações): [descrição]
    - Continuidade sem HA (backup/restauro): [RPO/RTO orientativos]
    - Suporte (níveis/horários, tempos de resposta iniciais): [descrição]
    - Custos (compute, storage, rede, comunicações, egress, operação, FinOps): [€ + notas]
  - CLOUD Backup
    - Frequência/retenção (>= diário; >=30 dias): [descrição]
    - Segregação (conta/subscrição/tenant distinto; WORM; residência UE): [descrição]
    - Segurança (AES-256; TLS >= 1.2; checksums): [descrição]
    - Testes de restauro (periodicidade; evidências): [descrição]
    - Custos (armazenamento; operações; retenção; testes; operação): [€ + notas]
  - DATAHUB
    - Ingestão (batch/stream), catálogo/lineage, qualidade/governação: [descrição]
    - APIs (operacional vs exploratória; latências típicas): [descrição]
    - BI/analítica/IA; partilha interna/dados abertos (RGPD): [descrição]
    - Interoperabilidade (formatos abertos; REST/GraphQL; K8s/containers; IaC): [descrição]
    - Backup do DataHub (segregado; encriptado; RPO/RTO; testes): [descrição]
    - Custos (ingestão, armazenamento/processamento, APIs, metadados,

operação/FinOps): [€ + notas]
        - Custos do backup do DataHub: [€ + notas]
    - DR EM CLOUD (ON-PREM CRÍTICOS)
        - Sistemas críticos (lista c.2.1 / c.2.2): [lista]
        - Replicação/sincronização (contínua/periódica): [descrição]
        - Failover orquestrado (por sistema/total/parcial): [descrição]
        - RTO (ativação) e testes (semestrais): [descrição]
        - Segurança/conformidade (RGPD/NIS2/ISO; residência UE): [descrição]
        - Custos (replicação; storage; testes; operação): [€ + notas]
- **Plano de implementação (marcos): [cronograma]**
- **Formação e Transferência de conhecimento**
    - Plano de transferência de conhecimento: [resumo]
    - Perfis (básico/analista/avançado) e conteúdos: [plano]
    - Modalidade (presencial/remota/híbrida); materiais: [descrição]
    - Shadowing/handover; objetivo de autonomia da equipa CML: [meta por ano]
- **OPERAÇÃO & SUPORTE (4 ANOS)**
    - Modelo de operação 24/7; monitorização; gestão de incidentes: [descrição]
    - Relatórios mensais (desempenho, segurança, custos): [descrição]
    - SLA de resposta inicial (objetivo, p.ex. <= 4h): [descrição]
    - Runbooks operacionais (backup/restauro; DR; pipelines; APIs): [lista]
- **FINOPS**
    - Ferramentas/processos (previsão, otimização, alertas): [descrição]
    - Otimização e tagging obrigatório para chargeback/showback (esquema): [descrição]
    - Limiares de alerta; reporte mensal (custos/uso): [descrição]
- **PORTABILIDADE & EXIT**
    - Exportação de dados (formatos abertos; metadados/lineage): [descrição]
    - Portabilidade de artefactos (IaC; contentores/orquestração): [descrição]
    - Passos/tempos/custos de exit (entre clouds ou retorno on-prem): [estimativa]
- **TCO 4 anos (resumo): [€], detalhando:**
    - Licenças/subscrições em conformidade com os itens descritos na alínea j) do ponto 4.1.7 (Cloud, DataHub, SGBD (incluindo oracle), segurança, API Mgmt): [€]
    - Serviços de migração: [€]
    - Operação/suporte (24/7, monitorização, relatórios): [€]
    - Backup (armazenamento, operações, testes/restauros): [€]
    - DR on-prem (replicação, storage, testes): [€]
    - Egress (volume + €/GB): [detalhe/mês]
    - Comunicações (VPN/interconexão + latências): [€]

  - Ferramentas/serviço FinOps: [€]
  - Formação & transferência de conhecimento: [€]
- **Vantagens técnicas: [descrição]**
- **Riscos/limitações: [descrição]**
- **Garantias aplicáveis: [lista]**
- **Assunções/dependências/exclusões: [lista]**

5.2 REQUISITOS SAAS/PAAS

Preenchimento do Anexo A relativo aos requisitos SaaS/PaaS, que se encontra em Anexo.

5.3 APRESENTAÇÃO DE SUMÁRIO EXECUTIVO

Documento em formato máximo de 3 páginas, para cada solução dos **Modelos A e B** que inclua:

- **Arquitetura de alto nível**: componentes e interações (Cloud, Cloud Backup, DataHub, DR on-prem, conectividade e segurança).
- **Plano de implementação**: marcos e duração indicativa; garantias aplicáveis.
- **Plano de transferência de conhecimento** (objetivo de autonomia da CML).
- **Estimativa de custos para 4 anos (TCO)**: licenças/subscrições (descriminado os diversos componentes)+ serviços + egress + comunicações + operação/FinOps.
- **Vantagens técnicas e financeiras**
- **Riscos/limitações** (em pontos).
- **Assunções, dependências e exclusões**.

Anexo A – Requisitos para Fornecedores de Soluções PaaS / SaaS

Neste documento encontram-se elencados um conjunto de requisitos a ter em conta na resposta à presente Consulta Preliminar. Os fornecedores devem responder em cada célula com:

1. Sim: a solução que apresentam cumpre o requisito

2. Não: a solução que apresentam não cumpre o requisito

3. Não Aplicável: não tem sentido aplicar este requisito à solução que apresentam.

1. Requisitos de Segurança e Conformidade da Solução			
1.1 Autenticação e Autorização **1.1.1 Protocolo OAuth 2.0**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AA.01	A solução implementa o protocolo OAuth 2.0, RFC 5849 e atualizações, com fluxo de código de autorização (authorization code flow).		
REQ.AA.02	A solução suporta o fluxo de credenciais do cliente (client credentials flow).		
REQ.AA.03	A solução suporta o mecanismo de revogação previsto no RFC 7009.		
REQ.AA.04	A solução suporta tokens de atualização (refresh tokens) com tempo de vida configurável.		

1. Requisitos de Segurança e Conformidade da Solução			
1.1 Autenticação e Autorização **1.1.2 Integração com Sistemas de Identidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AA.05	A solução integra com o fornecedor de identidade da CML via SAML 2.0.		
REQ.AA.06	A solução suporta autenticação via OpenID Connect.		
REQ.AA.07	A solução implementa a autenticação através da Chave Móvel Digital.		
REQ.AA.08	A solução suporta autenticação multifator (Multi-Factor Authentication).		

1. Requisitos de Segurança e Conformidade da Solução			
1.1 Autenticação e Autorização **1.1.3. Gestão de Permissões**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AA.09	A solução implementa controlo de acesso baseado em funções (Role-Based Access Control).		
REQ.AA.10	A solução suporta controlo de acesso baseado em atributos (Attribute-Based Access Control).		
REQ.AA.11	A solução permite a delegação temporária de acessos com validade configurável.		
REQ.AA.12	A solução implementa segregação de funções para operações críticas.		

1. Requisitos de Segurança e Conformidade da Solução			
1.1 Autenticação e Autorização **1.1.4 Integração com Microsoft Entra ID**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AA.13	A solução suporta autenticação através do Microsoft Entra ID (anteriormente Azure AD) utilizando o protocolo OpenID Connect.		
REQ.AA.14	A solução sincroniza e utiliza os grupos do Microsoft Entra ID para gestão de permissões.		
REQ.AA.15	A solução suporta mapeamento configurável entre grupos do Entra ID e permissões da aplicação.		
REQ.AA.16	A solução atualiza automaticamente as permissões quando houver alterações nos grupos do Entra ID.		
REQ.AA.17	A solução suporta grupos encadeados (nested groups) do Entra ID.		
REQ.AA.18	A solução permiti a utilização de evidências (claims) do Entra ID para atributos do utilizador.		

1. Requisitos de Segurança e Conformidade da Solução			
1.1 Autenticação e Autorização **1.1.5 Auditoria e Monitorização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AA.19	A solução regista todas as tentativas de autenticação, sucedidas ou falhadas.		
REQ.AA.20	A solução mantém um histórico completo de alterações de permissões.		
REQ.AA.21	A solução gera alertas para tentativas de acesso suspeitas.		
REQ.AA.22	A solução fornece relatórios detalhados de atividade de autenticação.		

1.Requisitos de Segurança e Conformidade da Solução			
1. 1 Autenticação e Autorização **1.1.6 Proteção e Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AA.23	A solução implementa proteção contra ataques de força bruta (brute force).		
REQ.AA.24	A solução bloqueia contas após número configurável de tentativas falhadas.		
REQ.AA.25	A solução força a alteração de palavras-passe temporárias no primeiro acesso.		
REQ.AA.26	A solução valida a força das palavras-passe segundo política configurável.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.01	A solução adota os princípios necessários ao cumprimento do Regulamento Geral de Proteção de Dados (RGPD), **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016** e respetiva Lei de Execução Nacional (Lei n.º		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	58/2019, de 8 de agosto).		
REQ.PD.02	A solução implementa os requisitos técnicos definidos na Resolução do Conselho de Ministros n.º 41/2018 (arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais).		
REQ.PD.03	O fornecedor demonstra conformidade com as deliberações e orientações da CNPD aplicáveis ao setor público.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.1 - Conformidade RGPD**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.04	O fornecedor prepara e fornece todos os elementos necessários ao cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD [conforme alínea f) do art.º 28.º do RGPD] e celebra um Acordo de Tratamento de Dados nos termos definidos pela CML em sede de assinatura de contrato.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.2 - API de Proteção de Dados**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.05	A solução fornece uma API REST documentada para execução de ações relacionadas com o cumprimento do RGPD.		
REQ.PD.06	A solução disponibiliza através da API endpoints específicos para: • Pedido de acesso aos dados (right of access) • Pedido de eliminação de dados (right to		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.2 - API de Proteção de Dados**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	erasure) · Pedido de portabilidade de dados (right to data portability) · Pedido de retificação de dados (right to rectification) · Gestão de consentimentos (consent management) · Limitação do tratamento (right to restriction of processing)		
REQ.PD.07	A solução retorna através da API o estado e progresso de cada pedido RGPD.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.3 Encriptação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.08	A solução utiliza TLS 1.3 ou superior para todas as comunicações em rede.		
REQ.PD.09	Todos os certificados utilizados são emitidos por uma Autoridade de Certificação (CA) conhecida.		
REQ.PD.10	A solução implementa encriptação em repouso (encryption at rest) utilizando AES-256 e modos de operação seguros (como o CBC ou GCM).		
REQ.PD.11	A solução suporta a gestão de chaves de encriptação através de um sistema de gestão de chaves (key management system).		
REQ.PD.12	A solução roda automaticamente as chaves de encriptação segundo política configurável.		
REQ.PD.13	A solução encripta dados sensíveis em registos de auditoria (audit logs).		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.4 Exportação e Portabilidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.14	A solução mantém um registo detalhado de todas as operações de exportação de dados.		
REQ.PD.15	A solução implementa limites configuráveis para operações de exportação em massa.		
REQ.PD.16	A solução inclui assinaturas digitais nas exportações de dados para garantir integridade.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.5 Auditoria e Rastreabilidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.17	A solução regista todos os acessos a dados pessoais, incluindo visualizações.		
REQ.PD.18	A solução mantém um histórico completo de alterações a dados pessoais (change tracking).		
REQ.PD.19	A solução incluí a finalidade do processamento em todos os registos de auditoria.		
REQ.PD.20	A solução permite a pesquisa e filtragem avançada nos registos de auditoria.		
REQ.PD.21	A solução preserva os registos de auditoria por um período configurável.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.6 Isolamento e Segmentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.22	A solução implementa segregação lógica de dados entre diferentes clientes (multitenancy).		
REQ.PD.23	A solução suporta a definição de políticas de retenção por tipo de dados.		

1. Requisitos de Segurança e Conformidade da Solução			
1.2 Proteção de Dados **1.2.6 Isolamento e Segmentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.PD.24	A solução implementa controlos de acesso ao nível do campo (field-level security).		
REQ.PD.25	A solução permite a classificação de dados segundo níveis de sensibilidade.		
REQ.PD.26	A solução aplica políticas de proteção baseadas na classificação dos dados.		
REQ.PD.27	A solução está toda sediada dentro da União Europeia e não permite o armazenamento nem qualquer fluxo transfronteiriço de dados para países terceiros ou organizações internacionais.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.01	A solução cumpre com os requisitos do Regime Jurídico de Segurança do Ciberespaço (Leis n.º 46/2018 e n.º 65/2021) para operadores de serviços essenciais, bem como com as suas revisões futuras, em particular com a transposição da diretiva SRI 2 (NIS 2) para a lei nacional.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.1 Gestão de Incidentes**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.02	O fornecedor implementa mecanismos de deteção e notificação de incidentes de segurança.		
REQ.SC.03	O fornecedor fornece toda a informação necessária para notificação ao CNCS em caso de incidente.		
REQ.SC.04	O fornecedor mantém um registo detalhado de todos os incidentes de segurança, incluindo tentativas de intrusão.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.1 Gestão de Incidentes**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.05	O fornecedor suporta a categorização de incidentes segundo a taxonomia definida pelo CNCS/CERT.PT.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.2 Monitorização Contínua**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.06	O fornecedor implementa monitorização contínua de segurança (continuous security monitoring).		
REQ.SC.07	A solução integra com o SIEM da CML através de API ou protocolo normalizado a definir durante a implementação da solução.		
REQ.SC.08	O fornecedor gera alertas em tempo real para atividades suspeitas.		
REQ.SC.09	A solução fornece métricas de segurança alinhadas com os requisitos do RJSC (Regime Jurídico de Segurança do Ciberespaço).		
REQ.SC.10	A solução suporta a realização de verificações periódicas de segurança (security assessments).		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.3 Controlos de Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.11	A solução implementa todos os controlos de segurança obrigatórios definidos no RJSC.		
REQ.SC.12	A solução suporta autenticação forte (strong authentication) para todas as contas privilegiadas.		
REQ.SC.13	A solução mantém registos de auditoria (audit logs) num formato não repudiável.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.3 Controlos de Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.14	A solução implementa mecanismos de proteção contra ataques conhecidos (known attack patterns).		
REQ.SC.15	A solução garante a segmentação de redes conforme as melhores práticas do RJSC.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.4 Relatórios e Documentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.16	A solução gera relatórios de conformidade com o RJSC automaticamente.		
REQ.SC.17	A solução mantém um inventário atualizado de todos os ativos de informação.		
REQ.SC.18	O fornecedor documenta todas as medidas de segurança implementadas.		
REQ.SC.19	O fornecedor fornece evidências para auditorias de conformidade com o RJSC.		
REQ.SC.20	O fornecedor mantém registos de todas as avaliações de risco realizadas.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.5 Gestão de Vulnerabilidades**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.21	A solução implementa proteções contra-ataques comuns, como: • Cross-Site Scripting (XSS); • Cross-Site Request Forgery (CSRF); • SQL Injection; • Session Hijacking.		

1. Requisitos de Segurança e Conformidade da Solução			
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.5 Gestão de Vulnerabilidades**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SC.22	A solução suporta a realização de análises regulares de vulnerabilidades.		
REQ.SC.23	O fornecedor implementa processo formal de gestão de vulnerabilidades.		
REQ.SC.24	A solução permite a integração com ferramentas de análise de vulnerabilidades da CML.		
REQ.SC.25	A solução mantém um registo do estado de correção das vulnerabilidades identificadas.		
REQ.SC.26	A solução prioriza a correção de vulnerabilidades segundo critérios do RJSC.		

1. Requisitos de Segurança e Conformidade da Solução			
1.4 Armazenamento **1.4.1 Proteção de Cópias de Segurança (Backups)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AS.01	A solução encripta todas as cópias de segurança.		
REQ.AS.02	A solução armazena os backups em localização física distinta dos dados primários.		
REQ.AS.03	A solução implementa controlo de acesso baseado em funções para operações de backup.		
REQ.AS.04	A solução mantém registos de auditoria de todas as operações de backup e restauro.		
REQ.AS.05	A solução verifica a integridade dos backups através de checksums criptográficos.		

1. Requisitos de Segurança e Conformidade da Solução			
1.4 Armazenamento **1.4.2 Gestão de Dados Sensíveis**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AS.06	A solução suporta máscaras de dados (data masking) para ambientes não produtivos.		
REQ.AS.07	A solução implementa controlos especiais para dados pessoais sensíveis.		
REQ.AS.08	A solução mantém registos de localização de todos os dados sensíveis.		
REQ.AS.09	A solução implementa mecanismos de eliminação segura de dados (secure deletion).		
REQ.AS.10	A solução suporta diferentes políticas de retenção baseadas na sensibilidade dos dados.		

2. Requisitos Operacionais			
2.1 Disponibilidade e Resiliência **2.1.1 Recuperação de Desastres**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DR.01	A solução suporta pontos de restauro (recovery points) configuráveis, com período mínimo de 30 dias.		
REQ.DR.02	A solução realiza testes automáticos periódicos dos procedimentos de recuperação.		
REQ.DR.03	A solução mantém um registo detalhado (audit log) de todas as operações de recuperação executadas.		
REQ.DR.04	A solução valida a integridade dos dados após cada operação de recuperação.		

2. Requisitos Operacionais			
2.2 Monitorização **2.2.1 Monitorização da Disponibilidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.MO.01	A solução fornece métricas em tempo real sobre o estado de disponibilidade do serviço.		
REQ.MO.02	A solução implementa alertas automáticos para falhas de disponibilidade que excedam limiares configuráveis.		
REQ.MO.03	A solução mantém histórico de disponibilidade com granularidade mínima de 5 minutos.		

2. Requisitos Operacionais			
2.2 Monitorização **2.2.2 Alarmística**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.MO.04	A solução implementa sistema de alertas para eventos críticos com suporte para múltiplos canais de notificação.		
REQ.MO.05	A solução permite a definição de limiares (thresholds) configuráveis para geração de alertas.		
REQ.MO.06	A solução suporta agregação de alertas para evitar sobrecarga de notificações.		
REQ.MO.07	A solução implementa mecanismo de escalamento (escalation) de alertas baseado em regras configuráveis.		

2.Requisitos Operacionais			
2.2 Monitorização **2.2.3 Dashboards e Visualização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.MO.08	A solução fornece painéis de controlo (dashboards) pré-configurados para monitorização da solução.		
REQ.MO.09	A solução permite visualizar, em dashboard, as métricas de desempenho dos diferentes serviços e		

2.Requisitos Operacionais			
2.2 Monitorização **2.2.3 Dashboards e Visualização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	integrações.		
REQ.MO.10	A solução permite a exportação de dados de monitorização em formatos standard (CSV, JSON).		

2. Requisitos Operacionais			
2.3 Suporte e Manutenção **2.3.1 Suporte Técnico**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SM.01	A solução SaaS integra com o sistema de gestão de pedidos (tickets) da CML, a definir durante a fase de implementação.		
REQ.SM.02	O sistema de gestão de pedidos da CML recebe todos os pedidos de suporte referentes à solução.		
REQ.SM.03	O fornecedor disponibiliza suporte técnico em português de Portugal durante o horário laboral (9h-18h).		
REQ.SM.04	O fornecedor alimenta a base de conhecimento (knowledge base) da CML com soluções para problemas comuns.		
REQ.SM.05	O fornecedor disponibiliza um canal de suporte prioritário para incidentes críticos com disponibilidade 24x7.		
REQ.SM.06	Os pedidos de suporte são classificados nas prioridades: Baixa, Alta, Muito Alta e Crítica.		

2. Requisitos Operacionais			
2.3 Suporte e Manutenção **2.3.2 Níveis de Serviço**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SM.07	A solução tem um Acordo de Nível de Serviço Service Level Agreement (SLA) que especifique: • Tempo máximo de resposta para incidentes críticos. • Tempos máximos de resolução por tipo de incidente. • Disponibilidade mínima mensal do serviço de _____%. **(indicar o valor percentual da solução proposta).**		
REQ.SM.08	O fornecedor disponibiliza um portal onde a CML possa consultar em tempo real: • Estado atual do serviço. • Histórico de disponibilidade. • Registo de incidentes e tempos de resolução. • Cálculo automático de penalizações.		
REQ.SM.09	Os pedidos de suporte de prioridade Baixa têm: **(indicar os valores da solução proposta).** • Tempo de resposta máximo é de _____ horas úteis. • Tempo de resolução máximo é de _____ dias úteis.		
REQ.SM.10	Os pedidos de suporte de prioridade Alta têm: **(indicar os valores da solução proposta).** • Tempo de resposta máximo é de _____ horas úteis. • Tempo de resolução máximo de _____ dias úteis.		
REQ.SM.11	Os pedidos de suporte de prioridade Muito Alta têm: **(indicar os valores da solução proposta).** • Tempo de resposta máximo de _____ horas úteis. • Tempo de resolução máximo de _____ horas úteis.		
REQ.SM.12	Os pedidos de suporte de prioridade Crítica terão: **(indicar os valores da solução proposta).** • Tempo de resposta máximo de _____ horas úteis. • Tempo de resolução máximo de _____ horas úteis.		

2. Requisitos Operacionais			
2.3 Suporte e Manutenção **2.3.3 Gestão de Atualizações**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SM.13	A solução fornece um plano de gestão de alterações (change management) documentado para todas as atualizações.		
REQ.SM.14	A solução notifica com antecedência mínima de 15 dias sobre atualizações planeadas que afetem a integração.		
REQ.SM.15	A solução mantém um ambiente de testes atualizado para validação de alterações antes da implementação em produção.		
REQ.SM.16	A solução fornece procedimentos de retrocesso (rollback) documentados para todas as atualizações.		

2. Requisitos Operacionais			
2.3 Suporte e Manutenção **2.3.4 Manutenção Preventiva**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SM.17	A solução executa verificações preventivas periódicas dos mecanismos de sincronização.		
REQ.SM.18	A solução realiza análises regulares de desempenho e capacidade.		
REQ.SM.19	A solução fornece recomendações proativas para otimização da integração.		
REQ.SM.20	A solução mantém um calendário de manutenção preventiva acordado com a CML.		

3. Documentação Requerida			
3.1 Documentação Técnica **3.1.1 Especificação de API**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DT.01	O fornecedor entrega documentação completa das API em formato OpenAPI 3.0 ou superior, incluindo todos os endpoints, respostas, metadados, modelos de dados e exemplos de utilização.		
REQ.DT.02	O fornecedor fornece documentação detalhada dos mecanismos de autenticação e autorização implementados.		
REQ.DT.03	O fornecedor documenta todos os limites de taxa de utilização (rate limits) e quotas aplicáveis às API.		
REQ.DT.04	A solução mantém um catálogo atualizado de todos os serviços e interfaces disponíveis.		

3.Documentação Requerida			
3.1 Documentação Técnica **3.1.2 Arquitetura e Fluxos**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DT.05	O fornecedor fornece diagramas de arquitetura detalhados em formato padrão UML ou C4 Model, ilustrando todos os componentes do sistema.		
REQ.DT.06	O fornecedor documenta todos os fluxos de dados entre o sistema SaaS e a plataforma da CML, incluindo diagramas de sequência.		
REQ.DT.07	O fornecedor fornece documentação sobre a topologia de rede necessária para a integração, incluindo requisitos de firewall e portos de comunicação.		

3. Documentação Requerida			
3.1 Documentação Técnica **3.1.3 Modelos de Dados**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DT.08	O fornecedor documenta o modelo de dados completo, identificando claramente as entidades consideradas estratégicas ou de alto valor.		
REQ.DT.09	O fornecedor fornece mapeamentos (mappings) detalhados entre o modelo de dados completo e o modelo simplificado para replicação.		
REQ.DT.10	O fornecedor documenta todas as restrições de integridade referencial e regras de negócio aplicáveis aos dados estratégicos.		

3. Documentação Requerida			
3.1 Documentação Técnica **3.1.4 Mecanismos de Sincronização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DT.11	O fornecedor documenta detalhadamente os mecanismos de sincronização implementados, incluindo gestão de conflitos.		
REQ.DT.12	O fornecedor documenta os mecanismos de validação e garantia de integridade dos dados sincronizados.		

3. Documentação Requerida			
3.1 Documentação Técnica **3.1.5 Monitorização e Diagnóstico**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DT.13	O fornecedor fornece documentação detalhada sobre os registos (logs) gerados pelo sistema, incluindo formato e estrutura.		
REQ.DT.14	O fornecedor documenta procedimentos de diagnóstico e resolução para cenários comuns de problemas.		

3.Documentação Requerida			
3.1 Documentação Técnica **3.1.6 Migração e Transição**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DT.15	O fornecedor fornece documentação detalhada dos procedimentos de migração de dados.		
REQ.DT.16	O fornecedor documenta o plano de transição para cenários de término de contrato.		
REQ.DT.17	O fornecedor fornece documentação sobre os procedimentos de exportação de dados em formatos padrão da indústria.		

3. Documentação Requerida			
3.2 Documentação Operacional **3.2.1 Procedimentos de Recuperação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DO.01	O fornecedor entrega um plano detalhado de recuperação de desastres (disaster recovery) que inclua: • Procedimentos passo-a-passo; • Responsabilidades e papéis; • Tempos máximos de recuperação Recovery Time Objective (RTO); • Pontos de recuperação garantidos Recovery Point Objective (RPO).		
REQ.DO.02	O fornecedor fornece documentação dos procedimentos de restauro (restore) de dados estratégicos.		
REQ.DO.03	O fornecedor documenta os procedimentos de verificação pós-recuperação.		

3. Documentação Requerida			
3.2 Documentação Operacional **3.2.2 Planos de Contingência**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DO.04	O fornecedor documenta planos de contingência para cenários críticos, incluindo: • Falhas de conectividade • Corrupção de dados • Comprometimento de segurança • Indisponibilidade de serviço		
REQ.DO.05	O fornecedor DEVE documentar procedimentos alternativos para operação em modo degradado.		

3. Documentação Requerida			
3.2 Documentação Operacional **3.2.3 Resolução de Problemas**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DO.06	O fornecedor fornece guias de resolução de problemas (troubleshooting) com: • Cenários comuns de erro; • Procedimentos de diagnóstico; • Soluções recomendadas; • Árvores de decisão para resolução.		
REQ.DO.07	O fornecedor documenta procedimentos de recolha de informação de diagnóstico.		

3.Documentação Requerida			
3.2 Documentação Operacional **3.2.4 Procedimentos de Suporte**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DO.08	O fornecedor documenta os processos de suporte, incluindo: • Canais de comunicação • Horários de atendimento; • Tempos de resposta por severidade;		

3.Documentação Requerida			
3.2 Documentação Operacional **3.2.4 Procedimentos de Suporte**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	• Procedimentos de escalamento.		
REQ.DO.09	O fornecedor fornece documentação sobre os procedimentos de manutenção preventiva.		
REQ.DO.10	O fornecedor documenta os processos de gestão de alterações (change management).		

3.Documentação Requerida			
3.2 Documentação Operacional **3.2.5 Monitorização Operacional**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DO.11	O fornecedor documenta os procedimentos de monitorização contínua do serviço.		
REQ.DO.12	O fornecedor fornece documentação sobre a interpretação de alertas e ações recomendadas.		
REQ.DO.13	O fornecedor documenta os procedimentos de geração de relatórios operacionais periódicos.		

3. Documentação Requerida			
3.2 Documentação Operacional **3.2.6 Segurança Operacional**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DO.14	O fornecedor documenta os procedimentos de resposta a incidentes de segurança.		
REQ.DO.15	O fornecedor fornece documentação sobre os procedimentos de gestão de acessos e credenciais.		
REQ.DO.16	O fornecedor documenta os procedimentos de auditoria de segurança periódica.		

4. Requisitos de Interface			
4.1 Requisitos técnicos			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IT.01	A interface web é compatível com as versões mais recentes dos seguintes navegadores para ambientes Desktop e para dispositivos Móveis: • Google Chrome; • Mozilla Firefox; • Microsoft Edge; • Safari.		
REQ.IT.02	A interface implementa mecanismos de cache adequados para otimizar o desempenho, seguindo as melhores práticas.		
REQ.IT.03	A interface suporta compressão de dados (gzip/deflate) para reduzir o volume de dados transferidos.		
REQ.IT.04	Os tempos de resposta da interface web respeitam os seguintes limites: • Carregamento inicial da página: máximo 2 segundos; • Operações interativas: máximo 1 segundo; • Apresentação de feedback visual: máximo 0.1 segundos.		
REQ.IT.05	A interface implementa gestão de sessões segura incluindo: • Timeout de inatividade configurável; • Invalidação segura de sessões; • Renovação segura de tokens.		
REQ.IT.06	A interface implementa validação de dados tanto no cliente como no servidor.		
REQ.IT.07	A interface implementa gestão adequada de erros com mensagens apropriadas para o utilizador.		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.1 Conformidade com Manual de Identidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IV.01	A solução implementa todas as diretrizes definidas no Manual de Normas Gráficas da Marca Lisboa, incluindo: • Logótipo e suas variantes;		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.1 Conformidade com Manual de Identidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	• Paleta de cores institucional; • Tipografia aprovada.		
REQ.IV.02	A solução utiliza apenas as cores definidas no manual de identidade, respeitando os códigos cromáticos especificados.		
REQ.IV.03	A conformidade visual será aferida pela CML e aprovada durante o desenvolvimento.		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.2 Personalização e Consistência**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IV.04	A solução permite a configuração de elementos visuais secundários mantendo a conformidade com as diretrizes principais.		
REQ.IV.05	A solução mantém consistência visual em todos os seus componentes, incluindo formulários, tabelas, botões e elementos interativos.		
REQ.IV.06	A solução implementa transições e animações de forma consistente em toda a interface.		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.3 Domínio e Apresentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IV.07	A solução utiliza exclusivamente o domínio web definido pela CML para todos os acessos públicos.		
REQ.IV.08	A solução apresenta elementos de marca (branding) conforme definido pela CML em: • Favicon; • Imagens de partilha em redes sociais;		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.3 Domínio e Apresentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	• Emails e notificações; • Documentos gerados.		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.4 Responsividade/Adaptabilidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IV.09	A solução mantém a integridade da identidade visual em todas as resoluções de ecrã e dispositivos.		
REQ.IV.10	A solução adapta elementos visuais mantendo a hierarquia e proporções definidas no manual de identidade.		
REQ.IV.11	A solução garante a legibilidade de todos os elementos visuais em diferentes tamanhos de ecrã.		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.5 Iconografia e Imagens**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IV.12	A solução utiliza apenas ícones aprovados pela CML ou que sigam as diretrizes de estilo definidas.		
REQ.IV.13	A solução implementa elementos decorativos e ilustrações conforme o estilo visual aprovado pela CML.		
REQ.IV.14	A solução mantém consistência no tratamento e estilo de imagens em toda a aplicação.		

4. Requisitos de Interface			
4.2 Identidade Visual **4.2.6 Versões e Atualizações**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IV.15	A solução suporta atualizações da identidade visual sem necessidade de reimplementação completa.		
REQ.IV.16	A solução permite a gestão de versões de elementos visuais, mantendo compatibilidade com versões anteriores quando necessário.		
REQ.IV.17	A solução fornece mecanismos para teste e validação de alterações visuais antes da sua implementação em produção.		

4. Requisitos de Interface			
4.3 Acessibilidade e Usabilidade **4.3.1 Conformidade com Normas**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IA.01	A solução cumpre as diretrizes de acessibilidade WCAG 2.1 nível AA como mínimo, de acordo com o portal acessibilidade.gov.pt.		
REQ.IA.02	A solução segue as normas europeias de acessibilidade EN 301 549.		
REQ.IA.03	A solução está em conformidade com o DL n.º 83/2018, referente à acessibilidade dos websites e das aplicações móveis.		

4. Requisitos de Interface			
4.3 Acessibilidade e Usabilidade **4.3.2 Navegação e Orientação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IA.04	A solução fornece múltiplos meios de localização dentro do conteúdo: • Navegação estruturada; • Função de pesquisa; • Mapa do site;		

4. Requisitos de Interface			
4.3 Acessibilidade e Usabilidade **4.3.2 Navegação e Orientação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	• Navegação baseada em breadcrumbs.		
REQ.IA.05	A solução mantém uma ordem de navegação lógica e consistente em todas as páginas.		
REQ.IA.06	A solução fornece indicações claras sobre a localização atual do utilizador na interface.		

4. Requisitos de Interface			
4.3 Acessibilidade e Usabilidade **4.3.3 Formulários e Interação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IA.07	A solução fornece etiquetas (labels) claras e instruções para todos os elementos de formulário.		
REQ.IA.08	A solução implementa validação de formulários com mensagens de erro claras e acessíveis.		
REQ.IA.09	A solução permite correção de erros de entrada com sugestões claras de resolução.		

4. Requisitos de Interface			
4.3 Acessibilidade e Usabilidade **4.3.4 Conteúdo Multimédia**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IA.10	A solução fornece alternativas textuais para todo o conteúdo não textual: • Descrições de imagens • Transcrições para áudio • Legendas para vídeo		
REQ.IA.11	A solução permite controlo de reprodução para conteúdo multimédia temporal.		
REQ.IA.12	A solução evita conteúdo com flash ou animações que possam causar convulsões.		

4. Requisitos de Interface			
4.3 Acessibilidade e Usabilidade **4.3.5 Desempenho e Resposta**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IA.13	A solução fornece feedback imediato para todas as ações do utilizador.		
REQ.IA.14	A solução implementa indicadores de progresso para operações longas.		
REQ.IA.15	A solução mantém tempos de resposta consistentes e previsíveis em toda a interface.		

4. Requisitos de Interface			
4.4 Internacionalização e Localização **4.4.1 Suporte Linguístico**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IL.01	A solução tem como idioma principal o português de Portugal.		
REQ.IL.02	A solução suporta o idioma inglês como idioma secundário.		
REQ.IL.03	A solução permite a alteração dinâmica do idioma sem necessidade de recarregamento da página.		
REQ.IL.04	A solução mantém o idioma selecionado entre sessões através de persistência de preferências.		
REQ.IL.05	A solução seleciona a língua a apresentar através das preferências indicadas pelo navegador do utilizador, usando o português por omissão.		

4. Requisitos de Interface			
4.4 Internacionalização e Localização **4.4.2 Interface e Documentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IL.06	A solução adapta automaticamente o layout para		

4. Requisitos de Interface			
4.4 Internacionalização e Localização **4.4.2 Interface e Documentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	acomodar diferentes comprimentos de texto entre idiomas.		
REQ.IL.07	A solução fornece toda a documentação de utilizador em português de Portugal.		
REQ.IL.08	A solução apresenta todas as mensagens de erro e avisos no idioma selecionado pelo utilizador, dentro dos disponíveis.		

4. Requisitos de Interface			
4.5 Integração com Sistemas CML **4.5.1 Autenticação e Autorização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IN.01	A solução utiliza a Chave Móvel Digital através da plataforma autenticacao.gov.pt para autenticação de utilizadores externos (munícipes).		
REQ.IN.02	A solução utiliza o Microsoft Entra ID para autenticação de utilizadores internos da CML.		
REQ.IN.03	A solução implementa um mecanismo de descoberta automática do tipo de utilizador para redireccionamento para o sistema de autenticação apropriado.		
REQ.IN.04	A solução mantém tokens de autorização separados para cada tipo de utilizador, respeitando os ciclos de vida específicos de cada sistema de autenticação.		

4. Requisitos de Interface			
4.5 Integração com Sistemas CML **4.5.2 Gestão de Sessões**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IN.05	A solução implementa tempos de sessão diferenciados: • Para utilizadores internos conforme política da CML; • Para utilizadores externos conforme regulamentação da autenticacao.gov.pt.		
REQ.IN.06	A solução sincroniza o estado da sessão com o serviço de autenticação correspondente.		
REQ.IN.07	A solução implementa terminação de sessão apropriada para cada tipo de autenticação.		

4. Requisitos de Interface			
4.5 Integração com Sistemas CML **4.5.3 Perfis e Permissões**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IN.08	A solução obtém de acesso dos utilizadores internos diretamente do Microsoft Entra ID.		
REQ.IN.09	A solução mantém uma estrutura de permissões própria apenas para utilizadores externos.		
REQ.IN.10	A solução valida e renova automaticamente as credenciais conforme as políticas de cada sistema de autenticação.		

4. Requisitos de Interface			
4.5 Integração com Sistemas CML **4.5.4 Ajuda e Suporte para Munícipes** Além dos fluxos de pedidos de suporte da CML para o fornecedor SaaS, deverá ser fornecida uma forma de receção de pedidos de suporte do munícipe referentes a funcionalidades da solução SaaS.			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IN.11	Em caso de pedido de suporte por parte dos munícipes a solução gera um novo email e envia		

4. Requisitos de Interface			
4.5 Integração com Sistemas CML **4.5.4 Ajuda e Suporte para Munícipes** Além dos fluxos de pedidos de suporte da CML para o fornecedor SaaS, deverá ser fornecida uma forma de receção de pedidos de suporte do munícipe referentes a funcionalidades da solução SaaS.			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	para o helpdesk@cm-lisboa.pt. O email deverá conter toda a informação necessária para a identificação da origem do pedido de suporte.		

4. Requisitos de Interface			
4.5 Integração com Sistemas CML **4.5.4 Ajuda e Suporte para Munícipes** Além dos fluxos de pedidos de suporte da CML para o fornecedor SaaS, deverá ser fornecida uma forma de receção de pedidos de suporte do munícipe referentes a funcionalidades da solução SaaS.			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IN.12	A solução pode vir a integrar com o sistema centralizado de ajuda da CML, a definir durante a fase de implementação da solução.		
REQ.IN.13	A solução pode vir a disponibilizar documentação de utilizador na base de conhecimento central da CML, a definir durante a fase de implementação da solução.		

5. Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.1 Certificações Gerais de Segurança da Informação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.01	A solução possuí certificação ISO/IEC 27001:2022 ou superior, ou compatível válida e emitida por entidade acreditada.		
REQ.CS.02	A solução mantém um Sistema de Gestão de Segurança da Informação (SGSI) alinhado com a ISO/IEC 27001 ou compatível.		
REQ.CS.03	O fornecedor disponibiliza à CML a declaração de aplicabilidade (Statement of Applicability) da		

5.Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.1 Certificações Gerais de Segurança da Informação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	certificação ISO/IEC 27001 ou compatível.		
REQ.CS.04	A solução possuí certificação SOC 2 Type II ou equivalente europeu, cobrindo os critérios de segurança, disponibilidade e confidencialidade.		
REQ.CS.05	A solução apresenta toda a infraestrutura de processamento e armazenamento de dados da CML fisicamente localizada em território da União Europeia, com proibição de transferência para jurisdições terceiras sem autorização expressa da CML.		

5.Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.2 Certificações Específicas para a Cloud**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.05	A infraestrutura cloud que suporta o sistema, possuí certificação ISO/IEC 27017 para segurança em cloud computing.		
REQ.CS.06	A infraestrutura cloud que suporta o sistema possuí certificação ISO/IEC 27018 para proteção de dados pessoais em cloud.		
REQ.CS.07	A infraestrutura cloud que suporta o sistema apresenta certificação CSA STAR (Security, Trust, Assurance, and Risk) nível 2 ou superior.		

5.Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.3 Conformidade com Normas de Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.08	A solução está em conformidade com as recomendações de segurança do Quadro Nacional de Referência para a Cibersegurança.		

5.Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.3 Conformidade com Normas de Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.09	O fornecedor demonstra conformidade com restantes recomendações de segurança do Centro Nacional de Cibersegurança (CNCS).		

5.Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.4 Validação e Manutenção de Certificações**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.10	O fornecedor realiza avaliações independentes de segurança (pen testing) por entidade certificada.		
REQ.CS.11	O fornecedor mantém um processo documentado de gestão contínua das certificações, incluindo renovações e atualizações.		
REQ.CS.12	O fornecedor notifica a CML com antecedência mínima de 90 dias sobre quaisquer alterações no estado das certificações.		

5. Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.5 Requisitos de Documentação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.13	O fornecedor disponibiliza toda a documentação comprovativa das certificações em português europeu ou inglês.		
REQ.CS.14	O fornecedor mantém um repositório atualizado com todos os relatórios de auditoria e certificação.		
REQ.CS.15	O fornecedor fornece relatórios periódicos de conformidade com as certificações (compliance reports).		

5. Conformidade e Certificações			
5.1 Conformidade e Certificações **5.1.6 Gestão de Incidentes e Continuidade**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CS.16	O fornecedor segue as indicações do ISO/IEC 27035 ou compatível para gestão de incidentes de segurança da informação.		
REQ.CS.17	A solução está em conformidade com a ISO 22301 ou compatível para gestão de continuidade de negócio.		
REQ.CS.18	O fornecedor mantém certificação ISO/IEC 27031 ou compatível para continuidade de negócio em TIC.		

6. Processo de Validação			
6.1 Ambientes de Validação **6.1.1 Disponibilização de Ambientes**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AV.01	O fornecedor disponibiliza um ambiente de testes dedicado que replique todas as funcionalidades do ambiente de produção.		
REQ.AV.02	O fornecedor mantém o ambiente de testes sincronizado com a versão de produção com diferença máxima de 5 dias úteis.		
REQ.AV.03	O fornecedor fornece um ambiente de validação com recursos dedicados e isolados de outros clientes.		

6. Processo de Validação			
6.1 Ambientes de Validação **6.1.2 Gestão de Dados de Teste**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AV.04	O ambiente de testes utiliza conjuntos de dados sintéticos que representem adequadamente os dados estratégicos.		

6. Processo de Validação			
6.1 Ambientes de Validação **6.1.2 Gestão de Dados de Teste**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AV.05	O fornecedor implementa um processo de refrescamento (refresh) periódico dos dados de teste que não utilize dados reais de produção.		
REQ.AV.06	O fornecedor fornece ferramentas para geração e manipulação de dados de teste que repliquem todos os cenários de integração.		

6. Processo de Validação			
6.1 Ambientes de Validação **6.1.3 Configuração de Ambientes**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AV.07	O fornecedor disponibiliza documentação detalhada da configuração necessária para estabelecer a ligação com o ambiente de testes.		
REQ.AV.08	O ambiente de testes suporta a simulação de todos os cenários de erro e exceção previstos nos requisitos de integração.		
REQ.AV.09	O fornecedor permite a reposição (reset) do ambiente de testes para um estado base conhecido em menos de _____ horas/dias. **(indicar o valor da solução proposta).**		

6. Processo de Validação			
6.1 Ambientes de Validação **6.1.4 Controlo de Acesso**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AV.10	O fornecedor implementa mecanismos de autenticação e autorização específicos para o ambiente de testes.		
REQ.AV.11	O fornecedor mantém um registo detalhado (audit log) de todas as operações realizadas no ambiente de testes.		

6. Processo de Validação			
6.1 Ambientes de Validação **6.1.4 Controlo de Acesso**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.AV.12	O fornecedor permite a gestão independente de utilizadores e permissões no ambiente de testes.		

6. Processo de Validação			
6.2 Testes Funcionais **6.2.1 Validação de Fluxos de Dados**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.TF.01	O fornecedor disponibiliza casos de teste documentados para cada fluxo de dados estratégicos identificado.		
REQ.TF.02	O fornecedor implementa validações automáticas para verificar a integridade dos dados durante os testes aos processos de sincronização.		
REQ.TF.03	O fornecedor fornece mecanismos de verificação da ordem cronológica das atualizações de dados estratégicos.		

6. Processo de Validação			
6.2 Testes Funcionais **6.2.2 Testes de Integração**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.TF.04	O fornecedor disponibiliza uma suite completa de testes de integração que cubra todos os endpoints da API.		
REQ.TF.05	O fornecedor fornece testes automatizados para validar o comportamento dos mecanismos de sincronização em modo offline.		
REQ.TF.06	O fornecedor implementa testes específicos para validar a gestão de conflitos na sincronização bidirecional.		

6. Processo de Validação			
6.2 Testes Funcionais **6.2.3 Validação de Transformações**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.TF.07	O fornecedor implementa testes automatizados para validar todas as transformações de dados entre o sistema SaaS e o modelo simplificado.		
REQ.TF.08	O fornecedor fornece casos de teste específicos para validar a preservação da integridade referencial após transformações.		
REQ.TF.09	O fornecedor disponibiliza ferramentas para comparação automatizada de dados antes e após transformações.		

6. Processo de Validação			
6.2 Testes Funcionais **6.2.4 Gestão de Estados**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.TF.10	O fornecedor fornece testes que validem a preservação do estado da aplicação durante falhas de conectividade.		
REQ.TF.11	O fornecedor implementa validações do processo de recuperação de estado após interrupções de sincronização.		
REQ.TF.12	O fornecedor disponibiliza testes para verificar a consistência dos dados em diferentes estados do sistema.		
REQ.TF.13	O fornecedor disponibiliza testes para verificar o funcionamento dos procedimentos de penalizações por indisponibilidade.		

6. Processo de Validação			
6.2 Testes Funcionais **6.2.5 Validação de Regras de Negócio**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.TF.14	O fornecedor implementa testes específicos para validar a aplicação das regras de classificação de dados estratégicos.		
REQ.TF.15	O fornecedor fornece casos de teste que validem as restrições de acesso aos dados estratégicos.		
REQ.TF.16	O fornecedor disponibiliza testes que verifiquem a correta aplicação das políticas de retenção de dados.		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.1 Análise de Vulnerabilidades**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.VS.01	O fornecedor realiza análises automáticas de vulnerabilidades em todo o código relacionado com a gestão de dados estratégicos.		
REQ.VS.02	O fornecedor executa verificações de segurança do código (code scanning) em todas as atualizações antes da implementação.		
REQ.VS.03	O fornecedor realiza análises regulares de vulnerabilidades nas bibliotecas e dependências utilizadas na integração.		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.2 Validação de Encriptação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.VS.04	O fornecedor valida a correta implementação dos mecanismos de encriptação em trânsito (in transit) através de testes automatizados.		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.2 Validação de Encriptação**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.VS.05	O fornecedor verifica a eficácia da encriptação em repouso (at rest) dos dados estratégicos através de testes de acesso direto ao armazenamento.		
REQ.VS.06	O fornecedor testa os procedimentos de rotação de chaves de encriptação sem impacto na disponibilidade dos dados.		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.3 Validação de Controlo de Acessos**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.VS.07	O fornecedor implementa testes automatizados para validar a correta aplicação das políticas de controlo de acesso.		
REQ.VS.08	O fornecedor garante e verifica a segregação efetiva de dados entre diferentes contextos de segurança.		
REQ.VS.09	O fornecedor testa a revogação imediata de acessos em todos os componentes da solução.		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.4 Auditoria de Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.VS.10	O fornecedor valida a completude e precisão dos registos de auditoria (audit logs) através de testes de rastreabilidade.		
REQ.VS.11	O fornecedor verifica a integridade dos registos de auditoria através de testes de manipulação.		
REQ.VS.12	O fornecedor testa os mecanismos de alerta de		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.4 Auditoria de Segurança**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	segurança através de simulações de incidentes.		
REQ.VS.13	A solução testa a preservação dos registos de auditoria por um período configurável.		
REQ.VS.14	A solução testa a exportação dos registos de auditoria em formato standard para análise externa.		

6. Processo de Validação			
6.3 Validação de Segurança **6.3.5 Testes de Resiliência**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.VS.15	O fornecedor realiza testes de continuidade de segurança durante falhas de componentes críticos.		
REQ.VS.16	O fornecedor valida o comportamento seguro do sistema durante a recuperação de falhas.		
REQ.VS.17	O fornecedor testa a preservação dos controlos de segurança durante operações em modo degradado.		

6. Processo de Validação			
6.4 Certificação de Integrações **6.4.1 Validação de API**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CI.01	O fornecedor valida a conformidade de todas as API expostas com a especificação OpenAPI 3.0 através de testes automatizados.		
REQ.CI.02	O fornecedor testa a implementação correta de todos os mecanismos de controlo de versão (versioning) das API.		

6. Processo de Validação			
6.4 Certificação de Integrações **6.4.1 Validação de API**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CI.03	O fornecedor verifica a correta implementação dos limites de pedidos (rate limiting) e quotas em todas as API.		

6. Processo de Validação			
6.4 Certificação de Integrações **6.4.2 Verificação de Protocolos**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CI.04	O fornecedor valida a conformidade com o protocolo OAuth 2.0 através de um conjunto completo de testes.		
REQ.CI.05	O fornecedor certifica a implementação correta do protocolo AMQP 1.0 para comunicações assíncronas.		
REQ.CI.06	O fornecedor verifica a conformidade com os protocolos de comunicação segura (TLS 1.3) através de testes específicos.		

6. Processo de Validação			
6.4 Certificação de Integrações **6.4.3 Validação de Sincronização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CI.07	O fornecedor certifica o funcionamento correto dos mecanismos de sincronização incremental.		
REQ.CI.08	O fornecedor valida a precisão dos registos temporais (timestamps) utilizados na sincronização.		
REQ.CI.09	O fornecedor garante a correta implementação dos mecanismos de deteção e resolução de conflitos.		

6. Processo de Validação			
6.4 Certificação de Integrações **6.4.4 Verificação de Formatos**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CI.10	O fornecedor valida a conformidade dos formatos de dados com os esquemas (schemas) JSON definidos.		
REQ.CI.11	O fornecedor certifica a correta codificação de caracteres (UTF-8) em todas as comunicações.		
REQ.CI.12	O fornecedor verifica a conformidade com os formatos de data e hora definidos na norma ISO 8601.		

6. Processo de Validação			
6.4 Certificação de Integrações **6.4.5 Certificação de Resiliência**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.CI.13	O fornecedor valida o comportamento das integrações durante falhas parciais do sistema.		
REQ.CI.14	O fornecedor verifica a recuperação automática das integrações após interrupções de conectividade.		
REQ.CI.15	O fornecedor certifica o correto funcionamento dos mecanismos de tentativas (retry) com espera exponencial.		

ANEXO A - COMPONENTE DE REPLICAÇÃO DE DADOS

A. Objetivo da Replicação Seletiva

A plataforma centralizada de dados da CML implementa uma estratégia de replicação seletiva, onde apenas os dados classificados como estratégicos são sincronizados e mantidos também nos sistemas da CML (on premises ou SaaS).

A replicação dos dados estratégicos ocorre na sua maioria no sentido do fornecedor para a plataforma centralizada de dados da CML. No entanto, neste caso é importante garantir a bidirecionalidade da replicação.

A replicação dos dados estratégicos tem como objetivos:

- Garantir a soberania sobre dados críticos;
- Facilitar a transição entre fornecedores;
- Otimizar custos de armazenamento e processamento;
- Simplificar a gestão de conformidade regulamentar;
- Garantia de operacionalidade mínima sem recurso a sistemas externos;
- Melhorar a eficiência da preservação digital.

B. Conceitos:

Dados Estratégicos

São considerados dados estratégicos aqueles que apresentam pelo menos uma das seguintes características:

- Dados essenciais para a continuidade operacional dos serviços municipais;
- Dados históricos necessários para análise e tomada de decisão;
- Dados que representam o registo oficial de interações com munícipes;
- Dados necessários para conformidade legal e regulamentar;
- Dados críticos para a transição entre fornecedores de serviços;
- Dados únicos ou de origem primária na CML, que se mantenham atuais.

Dados Não Estratégicos

São considerados dados não estratégicos:

- Dados operacionais temporários;
- Dados duplicados ou derivados de fontes primárias;
- Dados detalhados em cujos agregados sejam suficientes para análise e tomadas de decisão;
- Dados de configuração específicos da solução;
- Dados de utilização e métricas do sistema;
- Dados intermediários auxiliares resultantes de processamento.

Seguidamente, são elencados os requisitos para a "Componente de Replicação de Dados" para a Plataforma de Serviços de Lisboa, a saber:

7. Requisitos de Gestão de Dados Estratégicos			
7.1 Identificação e Classificação de Dados			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DE.01	O fornecedor fornece um catálogo dos dados armazenados pela solução.		
REQ.DE.02	O fornecedor documenta as dependências entre diferentes conjuntos de dados.		
REQ.DE.03	O fornecedor identifica claramente os dados necessários para a continuidade do negócio.		
REQ.DE.04	A CML irá definir junto do fornecedor aquilo que são dados estratégicos durante a fase de implementação.		
REQ.DE.05	A solução mantém um catálogo dos dados atualizado que inclua a sua classificação, período de retenção e dependências.		

7. Requisitos de Gestão de Dados Estratégicos			
7.2 Modelo de Dados Simplificado			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DE.06	A solução fornece um modelo de dados simplificado para os dados replicados que		

7. Requisitos de Gestão de Dados Estratégicos			
7.2 Modelo de Dados Simplificado			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	inclua apenas os atributos essenciais.		
REQ.DE.07	A solução incluí metadados essenciais para contextualização dos dados.		

7.Requisitos de Gestão de Dados Estratégicos			
7.3 Portabilidade e Interoperabilidade			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.DE.08	A solução armazena os dados estratégicos em formatos abertos e documentados.		
REQ.DE.09	A solução fornece APIs normalizadas para acesso aos dados estratégicos.		
REQ.DE.10	A solução incluí documentação completa do modelo para facilitar migrações futuras.		
REQ.DE.11	A solução permite a exportação dos dados em formatos standard da indústria.		
REQ.DE.12	A solução mantém um histórico das alterações ao modelo de dados.		
REQ.DE.13	A solução gera relatórios de exportação com meta-informação sobre o contexto dos dados.		
REQ.DE.14	A solução tem a funcionalidade de importar dados em lote já pré-existentes.		

7. Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.1 Interface Programática REST (obrigatória)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.01	A interface programática segue as especificações OpenAPI 3.0 ou superior		
REQ.IC.02	Incluí na descrição em OpenAPI meta informação		

7. Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.1 Interface Programática REST (obrigatória)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.03	Incluí na descrição em OpenAPI, para cada recurso (endpoint) as respostas possíveis.		
REQ.IC.04	Incluí na descrição em OpenAPI, os componentes reutilizáveis, incluindo os modelos de dados.		
REQ.IC.05	Produz as respostas de erro de acordo com o RFC 7807, Problem Details for HTTP APIs.		
REQ.IC.06	A interface programática utiliza JSON como formato de dados, em todas as situações.		
REQ.IC.07	A interface programática implementa autenticação e autorização com OAuth 2.0 (RFC 6749 e atualizações), mecanismos de autorização nativos do HTTP (RFC 7235), objetos JWT transportados em cabeçalho 'Authorization' ou através de chaves (keys) presentes noutros cabeçalhos HTTP, a definir durante a implementação da solução.		
REQ.IC.08	A interface programática suporta limites de taxa de utilização configuráveis (rate limiting).		
REQ.IC.09	A interface programática incluí a versão no URL (ex: <domínio>/v1/api/).		
REQ.IC.10	Suporta paginação.		
REQ.IC.11	Suporta filtragem sobre os atributos expostos nos modelos de dados.		

7.Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.1 Serviço de Notificações (Webhooks)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.12	O serviço permite subscrição de eventos específicos.		
REQ.IC.13	O serviço incluí assinatura digital das mensagens.		
REQ.IC.14	O serviço implementa nova tentativa (retry) com intervalos exponenciais em caso de falha.		

7.Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.1 Serviço de Notificações (Webhooks)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.15	O serviço suporta configuração de endpoints por ambiente.		

7.Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.2 Sistema de Publicação/Subscrição de Eventos (Pub/Sub)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.16	A solução utiliza o protocolo AMQP 1.0 ou superior.		
REQ.IC.17	A solução suporta filtros de eventos.		
REQ.IC.18	A solução permite configuração de qualidade de serviço (Quality of Service).		
REQ.IC.19	A solução implementa persistência de mensagens.		

7. Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.3 Exportação em Lote (Batch)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.20	A solução suporta paginação de resultados.		
REQ.IC.21	A solução permite filtragem por período temporal.		
REQ.IC.22	A solução implementa compressão de dados.		
REQ.IC.23	A solução suporta exportação incremental.		

7. Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.4 Conectores de Base de Dados**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.24	Os conectores suportam JDBC/ODBC para acesso direto aos dados.		
REQ.IC.25	Os conectores implementam agrupamento de ligações (connection pooling).		
REQ.IC.26	Os conectores permitem configuração de tempo limite em que as ligações estão abertas em idle (connection timeout).		
REQ.IC.27	Os conectores permitem configuração de tempo limite da execução de um comando (timeout).		
REQ.IC.28	Os conectores suportam TLS 1.3 para ligações seguras.		

7. Requisitos de Gestão de Dados Estratégicos			
7.4 Interfaces de Comunicação **7.4.5 Requisitos Comuns**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.IC.29	O mecanismo fornece documentação técnica completa em português de Portugal.		
REQ.IC.30	O mecanismo suporta monitorização através de métricas normalizadas.		
REQ.IC.31	O mecanismo implementa registo estruturado (logging) em formato JSON.		
REQ.IC.32	O mecanismo suporta rastreabilidade através de cabeçalhos de correlação.		
REQ.IC.33	Todas as interfaces de comunicação utilizam a sua versão mais segura, como por exemplo HTTPS (com TLS 1.3) em detrimento de HTTP.		

7. Requisitos de Gestão de Dados Estratégicos			
7.5 Sincronização de Dados O fornecedor implementa capacidades de sincronização que garantam a consistência dos dados entre o seu sistema e a plataforma central da CML. **7.5.1 Mecanismo de Sincronização Base**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SD.01	A solução replica para o datacentre da CML apenas os dados classificados como estratégicos.		
REQ.SD.02	A solução mantém um registo temporal (timestamp) da última atualização para cada registo.		
REQ.SD.03	A solução regista o momento temporal (timestamp) de cada operação de sincronização.		
REQ.SD.04	A solução implementa replicação incremental dos dados estratégicos.		
REQ.SD.05	A solução garante a ordem cronológica das atualizações.		
REQ.SD.06	A solução permite a configuração dos intervalos de sincronização por tipo de dados.		
REQ.SD.07	A solução mantém um registo detalhado de todas as operações de sincronização.		
REQ.SD.08	A solução calcula e verifica checksums para validar a integridade dos dados replicados.		
REQ.SD.09	A solução garante a consistência dos dados replicados através de validações periódicas.		
REQ.SD.10	A solução emite alertas em tempo real quando forem detetadas discrepâncias na sincronização.		

7. Requisitos de Gestão de Dados Estratégicos			
7.5 Sincronização de Dados **7.5.2 Operação em Modo Desligado (Offline)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SD.11	A solução mantém uma fila de alterações pendentes quando em modo desligado.		
REQ.SD.12	A solução sincroniza automaticamente as alterações pendentes quando a conectividade for restabelecida.		
REQ.SD.13	A solução implementa mecanismos de controlo de versões (versioning) para alterações em modo		

7. Requisitos de Gestão de Dados Estratégicos			
7.5 Sincronização de Dados **7.5.2 Operação em Modo Desligado (Offline)**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
	desligado.		
REQ.SD.14	A solução garante a consistência dos dados após sincronização de alterações em modo desligado.		
REQ.SD.15	A solução implementa mecanismo de nova tentativa (retry) com espera exponencial para todas as operações de sincronização falhadas.		

7.Requisitos de Gestão de Dados Estratégicos			
7.5 Sincronização de Dados **7.5.3 Controlo e Monitorização**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SD.16	A solução fornece métricas detalhadas sobre o processo de sincronização.		
REQ.SD.17	A solução emite notificações em caso de falhas de sincronização.		
REQ.SD.18	A solução mantém um registo detalhado (audit log) de todas as operações de sincronização.		
REQ.SD.19	A solução permite a configuração de limites de taxa de sincronização (throttling).		

7. Requisitos de Gestão de Dados Estratégicos			
7.5 Sincronização de Dados **7.5.4 Recuperação e Resiliência**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SD.20	A solução implementa mecanismos de nova tentativa (retry) com intervalos exponenciais em caso de falha.		
REQ.SD.21	A solução suporta pontos de verificação (checkpoints) para recuperação de sincronizações interrompidas.		

7. Requisitos de Gestão de Dados Estratégicos			
7.5 Sincronização de Dados **7.5.4 Recuperação e Resiliência**			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.SD.22	A solução mantém um histórico de estados anteriores para possibilitar reversão (rollback).		
REQ.SD.23	A solução implementa mecanismos de validação de integridade dos dados sincronizados.		

7. Requisitos de Gestão de Dados Estratégicos			
7.6 Formatos e Protocolos			
O fornecedor garante a conformidade com os formatos e protocolos padrão definidos pela CML para assegurar a interoperabilidade com a plataforma central.			
7.6.1 Compatibilidade Nacional			
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não/Não Aplicável)**	
		Cloud CML + Cloud Backup + Disaster Recovery	**DataHub + Backup Cloud**
REQ.FD.01	A solução suporta as diretivas da plataforma MOSAICO da AMA (Agência para a Modernização Administrativa).		
REQ.FD.02	A solução segue os princípios definidos no Regulamento Nacional de Interoperabilidade Digital (RNID).		